財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

18 April 2022

Chinese Taipei DESG Team
National Development Council

Mr Ekapong Rimcharone
Chair
Digital Economy Steering Group
Asia-Pacific Economic Cooperation

Mr Junichi Ishii
Chair
Data Protection Sub-Group
Asia-Pacific Economic Cooperation

Ms Shannon Coe
Chair
Joint Oversight Panel
Asia-Pacific Economic Cooperation

RE: APEC CBPR ACCOUNTABILITY AGENT RENEWAL APPLICATION SUBMISSION

1. The Institute for Information Industry ('III') is proud to have the opportunity to submit a renewal application to be an APEC recognized Accountability Agent under the APEC Cross Border Privacy Rules ('CBPR') System.
2. The III demonstrates that it continues to fulfil the requirements under *Annex A* of the *Accountability Agent APEC Recognition Application*.
3. The III is responsible for operating two systems – the domestic certification system and the APEC CBPRs certification system. In the initial application, the III mapped APEC requirements to its domestic certification system requirements and domestic personal information protection laws. In this renewal application, the III intends to continue this approach.
4. On 30 December 2021, the III issued a new set of domestic certification requirements ('NDCR'). The former set of domestic certification requirements ('FDCR') took effect in 2016. There is a two year grace period allowing organizations certified under the domestic certification system to transit into the NDCR. It is only reasonable to allow this grace period

to apply to APEC CBPRs certifications. Therefore, the III submits two sets of Program Requirements in this renewal application, as both will be used to assess organizations.

III PROGRAM REQUIREMENTS – CBPR: 2016

5. The III has mapped the FDCR and *the Personal Data Protection Act* to APEC requirements. This is the first set of Program Requirements submitted and is referred to as CBPR: 2016 in this renewal application. CBPR: 2016 was approved in the initial application and the content has not changed. The III will continue to use CBPR: 2016 to assess certain organizations that apply for APEC CBPRs certifications during the grace period.

III PROGRAM REQUIREMENTS – CBPR: 2021

6. The III has mapped the NDCR and *the Personal Data Protection Act* to APEC requirements. This is the second set of Program Requirements submitted and is referred to as CBPR: 2021 in this renewal application. The III intends to use CBPR: 2021 to assess organizations that apply for APEC CBPRs certifications which are not subject to the grace period.

ACCOUNTABILITY CASE NOTES & COMPLAINT STATISTICS

7. As the III has not begun APEC CBPRs certifications, there are no Case Notes or Complaint Statistics to report pursuant to *Annex D* and *Annex E* of the *Accountability Agent APEC Recognition Application*.

8. Please accept this renewal application. If you have any questions, please contact Steve Kuan Yu Lin, Section Manager at stevelin0330@iii.org.tw and Jasmine Chou, Associate Legal Researcher at jasminechou@iii.org.tw.
9. The III looks forward to continuing its role as an APEC recognized Accountability Agent.

Regards,

Cheng Hong Cho

Institute for Information Industry

APEC CBPR System Accountability Agent

RENEWAL APPLICATION

to apply to APEC CBPRs certifications. Therefore, the III submits two sets of Program Requirements in this renewal application, as both will be used to assess organizations.

III PROGRAM REQUIREMENTS – CBPR: 2016

5. The III has mapped the FDCR and *the Personal Data Protection Act* to APEC requirements. This is the first set of Program Requirements submitted and is referred to as CBPR: 2016 in this renewal application. CBPR: 2016 was approved in the initial application and the content has not changed. The III will continue to use CBPR: 2016 to assess certain organizations that apply for APEC CBPRs certifications during the grace period.

III PROGRAM REQUIREMENTS – CBPR: 2021

6. The III has mapped the NDCR and *the Personal Data Protection Act* to APEC requirements. This is the second set of Program Requirements submitted and is referred to as CBPR: 2021 in this renewal application. The III intends to use CBPR: 2021 to assess organizations that apply for APEC CBPRs certifications which are not subject to the grace period.

ACCOUNTABILITY CASE NOTES & COMPLAINT STATISTICS

7. As the III has not begun APEC CBPRs certifications, there are no Case Notes or Complaint Statistics to report pursuant to *Annex D* and *Annex E* of the *Accountability Agent APEC Recognition Application*.

8. Please accept this renewal application. If you have any questions, please contact Steve Kuan Yu Lin, Section Manager at stevelin0330@iii.org.tw and Jasmine Chou, Associate Legal Researcher at jasminechou@iii.org.tw.
9. The III looks forward to continuing its role as an APEC recognized Accountability Agent.

Regards,

Cheng Hong Cho

Table of Content

ENFORCABILITY

Is the Applicant subject to the jurisdiction of the relevant enforcement authority in a CBPR participating Economy?

The Institute for Information Industry (hereinafter referred to as "III") is a professional think tank and non-profit organization in Chinese Taipei. The III provides independent and impartial policies and technical services to governmental agencies, and operates the TPIPAS, a domestic certification system.[1]

The III is a public-endowed foundation established pursuant to law. Pursuant to the *Foundations Act* of Chinese Taipei, the III is supervised and governed by the Ministry of Economic Affairs, which is one of the Privacy Enforcement Authorities of Chinese Taipei (hereinafter referred to as "PEAs ").[2]

The III is Chinese Taipei's recognized APEC CBPR System Accountability Agent. The III has mapped FDCR, NDCR and the *Personal Data Protection Act* to the APEC CBPR Program Requirements, together they form the III's CBPR Program Requirements. The III ensures that all certified organizations comply with the III's CBPR Program Requirements. A description of how each of the Accountability Agent Recognition Criteria have been met using the Accountability Agent Recognition Criteria Checklist is as follows.

[1] For detailed information, please see the following link: https://www.tpipas.org.tw/.
[2] Please see the following link for the full text of the *Foundations Act*: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0020030

Conflicts of Interest

Q1: Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.

1. The III has imposed two internal regulations that aim to prevent conflicts of interest with respect to its employees (including members of the board of directors), and they are:

    a. the Working Rules, Code of Conducts, Ethical Management in Operating Procedures;

    b. the APEC CBPR Accountability Agent – Conflicts of Interest Policies and Procedures (hereinafter referred to as "Conflicts of Interest Policies and Procedures").

2. Pursuant to the Working Rules, Code of Conducts and the Ethical Management in Operating Procedures, if an III employee (including members of the board of directors) is subject to a conflicts of interest, he/she shall report and recuse himself/herself from the matter. The employee who fails to comply with the regulations will be punished.

3. The III has a three tiered supervisory structure when implementing the Conflicts of Interest Policies and Procedures. The Director General supervises the Director. The Director supervises the Executive Team. When an organization applies for APEC CBPRs certification, the Executive Team conducts a conflicts of interest check following the Conflicts of Interest Policies and Procedures. First, a member of the Executive Team must disclosure whether there is likely a conflicts of interest between the member and the organization, including its directors and employees. Secondly, the Executive Team reviews and determines whether there is likely a conflicts of interest between the organization and the III. Thirdly, the Executive Team reports its findings and decision to the Director, who conducts further review. Fourthly, the Director reports his/her findings and decision to the Director General. Finally, the Director General makes the final review and decision.

4. If there is a conflicts of interest, measures will be taken to avoid such conflict, including forbidding the employee to participate in the certification of that organization. If the conflict cannot be avoided, the III will cease to certify this organization. Employees who fail to comply with the III's internal regulations will be punished. Depending on whether it is a major or minor breach, the punishments include, termination of employment, job transfers, demotion, payment reductions, and performance appraisal being capped to a particular grade.

5. The III will not provide any counseling or technical services that may affect the III in performing its duties as an Accountability Agent (e.g., providing the consulting, examination and counseling services relating to personal information or information security to organizations that have applied for or have received APEC CBPRs certification from the III).

6. The III will publish information relating to the APEC CBPRs on a specific website (tpipas.org.tw), information include but is not limited to the III's CBPR Program Requirements and contact information. The statistics and abstracts of remarkable cases conducted according to the Guideline for the Operation of Dispute Resolution Mechanism of the Domestic Certification System will also be published on the website (please refer to Q9 to Q10).

7. The III will notify the Joint Oversight Panel (hereinafter referred to as "JOP") of conflicts of interest that result in a withdrawal or affiliations that might be on their face be considered a conflict of interest but did not result in a withdrawal.

8. The III will notify PEAs of Chinese Taipei of information related to certification of new organizations, audits of existing participant organizations, and dispute resolution.

Q2: Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.

(Please refer to Q1)

Q3: Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

(Please refer to Q1)

Program Requirements

Q4: Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.

The III submits two set of Program Requirements – CBPR:2016 and CBPR:2021. The III intends to make use of Annex C to map its existing intake procedures program requirements, which are FDCR, NDCR and the *Personal Data Protection Act* to requirements developed by APEC. The III intends to use the two sets of Program Requirements to assess organisations that have applied for APEC CBPRs certification.

The III will publish relevant documents on its Accountability Agent's website, along with links to the website of APEC CBPR for the reference of organizations applying for APEC CBPRs certification.

Certification Process

Q5: Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d) of Annex A have been met.

1. （Application）

1.1 An organization that applies for APEC CBPRs certification (hereinafter referred to as "Applicant Organization") shall submit the APEC CBPR Intake Questionnaire and application documents to the III, and shall pay relevant fees. The III and the Applicant Organisation is bound by a contract. The Applicant Organization may select the scope of certification.

1.2 The III will review if there are conflicts of interest between the III and the Applicant Organization as stated in Q1 to Q3.

2. （Written review）

2.1 The III certification team will review the documents submitted by the Applicant Organization and check if the documents comply with III Program Requirements.

2.2 After an Applicant Organization passes the written review, the III certification team will develop a certification plan, and will perform an on-site review in the offices of the Applicant Organization on a selected date. If the Applicant Organization fails the initial written review, it has one opportunity to rectify and correct, after which a fresh written review is to be conducted.

3. （On-site review）

3.1 The III will organize the main issues to be inspected during the on-site review according to the Intake Questionnaire and documents submitted by an Applicant Organization.

3.2 The methods of on-site review include, but are not limited to:

(1) Interview: the III certification team will inquire and certify relevant issues by personal interview, phone, e-mail, on-line meeting, *etc*.

(2) Observation: the III certification team will observe the procedures and processes relating to personal information, including but not limited to the effectiveness of the control and management and the security of information system of the procedures and processes relating to personal information.

(3) Random inspection: the III certification team will inspect relevant records and documents on a randomly selected basis, including but not limited to policies, documents, systems, websites, applications, *etc*.

3.3 After the completion of the on-site review, the III certification team will issue a formal report to explain if an Applicant Organization is in compliance with III Program Requirements.

3.4 If an Applicant Organization breaches III Program Requirements, the III will specify the breach in a formal report, and will ask the Applicant Organization to take corrective actions toward the breach within a certain period. III will confirm if the Applicant Organization completes the corrective actions and meets III Program Requirements. Only the Applicant Organizations that meet III Program Requirements will pass the APEC CBPRs certification. If the Applicant Organization fails the on-site review, it has one opportunity to rectify and correct, after which a fresh on-site review is to be conducted.

4. APEC CBPRs certification

4.1 The III will issue a certificate to Applicant Organizations that have passed APEC CBPRs certification, as evidence of becoming an organization that is certified under APEC CBPRs (“hereinafter referred to as “Certified Organization”).

4.2 The III will publish relevant information of Certified Organizations (including but not limited to the name, website, scope of certification or the term of certification of the Applicant Organizations) on the website of the Accountability Agent.

On-going Monitoring and Compliance Review Processes

Q6: Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).

(Please refer to Q7)

Q7: Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

1. To ensure that a Certified Organization meets III Program Requirements, within the term of its APEC CBPRs certification, the III may ask the Certified Organization to provide a written report or relevant information with respect to its personal information management system, and may conduct an on-site review, periodically or randomly, at the place of the Certified Organization if deemed necessary (the Certified Organization shall comply with directions from the III, and fees for the on-site review shall be borne by the Certified Organization).

2. If a Certified Organization encounters any of the following situations, it shall promptly notify the III in writing and provide relevant documents according to the request of III:

   (1) Material changes made or is likely going to be made to the personal information management system of the Certified Organization.

   (2) Types of services operated by the Certified Organization have changed.

   (3) Basic information of the Certified Organization specified in the application documents for APEC CBPRs certification have changed.

3. When a data breach occurs, the Certified Organization after making inquiries, shall promptly notify and provide a written report to the III as soon as possible. The report shall

specify the cause of the incident, the damage incurred from the incident, and how the incident is handled.

4. The III accepts complaints relating to Certified Organizations through its dispute resolution mechanism (please refer to Q9 to Q10), and has the power to investigate if Certified Organizations breaches III Program Requirements.

5. Upon breach of III Program Requirements, the III will ask the Certified Organization to rectify the breach within a certain period. The III has the power to suspend or terminate the Certified Organization's APEC CBPRs certification, prior to its rectification.

Re-Certification and Annual Attestation

Q8: Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d) of Annex A.

1. The III will carry out re-certification on the Certified Organization annually, to ensure that the Certified Organization complies with III Program Requirements.

2. A Certified Organization shall submit a re-certification application before its term of certification expires.

3. Please refer to Q5 for the procedures of re-certification. Procedures in relation to the submission of application documents, conflicts of interest, contract signing and written review may be streamlined. The assessment of program requirements may also be streamlined, the III certification team may select to review only areas that have changed since initial certification. Items being reviewed include, but are not limited to the following:

   (1) The Intake Questionnaires and application documents submitted by the Certified Organization.

   (2) The formal reports from the review of the preceding year.

   (3) The documents, procedures, processes and records relating to personal information.

4. If a Certified Organization breaches III Program Requirements, the III will specify the breach in a formal report, and will ask the Certified Organization to take corrective actions toward the breach within a certain period. The III will confirm if the Certified Organization completes the corrective actions and meets III Program Requirements. Only Certified Organizations that meet III Program Requirements will pass the annual APEC CBPRs recertification.

5. The III will issue a certificate to the Certified Organization that passed recertification as evidence of passing APEC CBPRs recertification.

6. If a Certified Organization has any of the following situations, the III may carry out an immediate review when necessary:

(1) Material changes made to the personal information protection policy, privacy policy or the business procedure of the Certified Organization.

(2) Complaints made against the Certified Organization via the dispute resolution mechanism (please refer to Q9 to Q10).

Dispute Resolution Process

Q9: Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognised Accountability Agents that may be used when appropriate.

1. The mechanism to receive and investigate complaints are governed under the *Guideline for the Operation of Dispute Resolution Mechanism of the Domestic Certification System*. This is the dispute resolution mechanism of the domestic certification system. The III adopts the same mechanism when operating the APEC CBPRs certification system. Details of the III's dispute resolution process is as follows:

    1.1 Receiving complaints and notification: Any person may file a complaint with the III, alleging that a Certified Organization breaches rules of the APEC CBPRs. The III will determine within seven working days. If the breach relates to compliance of APEC CBPRs rules, the III will notify the complainant and the Certified Organization in writing.

    1.2 Dispute investigation: The III shall complete the dispute investigation within one month after notifying the complainant and the Certified Organization. However, if the dispute is complicated and if necessary, the investigation period may be extended once. The III shall notify the complainant and the Certified Organization of the reasons for extension in writing. Methods of investigation include: (1) Ask the Certified Organization or the complainant to specify the details of the dispute; (2) Inquire the competent authority and the authority responsible for the legal interpretation of the *Personal Data Protection Act* to provide opinions. (3) Ask other APEC CBPRs Accountability Agents to assist. (4) Perform any other methods that is necessary to the investigation. If necessary for the investigation, the III may, after acquiring the consent of the complainant, provide his/her information to the Certified Organization.

1.3 Dispute resolution: The complainant and the Certified Organization shall be informed of the result of the dispute investigation in writing. If the Certified Organization is found in breach of APEC CBPRs rules, the Certified Organization shall rectify breaches within three months, and its APEC CBPRs certification will be suspended during this period. After the Certified Organization completes rectification, the III shall review and confirm if rectification is satisfactory, and shall notify the complainant and the Certified Organization. If the Certified Organization fails to complete the rectification within the period, its APEC CBPRs certification shall be terminated.

2. The III shall preserve information with respect to dispute resolution, compile the amount of disputes, types of disputes, the regulations involved and the handling of disputes, and publish them on the website of the domestic certification system. The III shall also notify the legal interpretation authority of the *Personal Data Protection Act* of Chinese Taipei and the JOP. The III shall publish the handling of remarkable complaints, including interpretation of regulations and suggestions to practical operation, on the website of the domestic certification system.

Q10: Applicant Accountability Agent should describe how the dispute resolution process meets the requirements identified in 10 (a) – (h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.

(Please refer to Q9)

Mechanism for Enforcing Program Requirements

Q11: Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.

If the Certified Organization breaches III Program Requirements, the III has the power to take actions listed in Q13 on the Certified Organization according to the regulations of the domestic certification system.

Q12: Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.

(Please refer to Q6 and Q7)

Q13: Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.

When a Certified Organization breaches III Program Requirements and fails to rectify the breach within a certain period, the III has the power to impose the following penalties:

(1) Warning the Certified Organization.

(2) Asking the Certified Organization to rectify the breach within a certain period. If the breach cannot be rectified, the III has the right to suspend or terminate the effect and use of the APEC CBPRs certification granted to the Certified Organization.

(3) Suspending the effect and use of the APEC CBPRs certification granted to the Certified Organization.

(4) Terminating the effect and use of the APEC CBPRs certification granted to the Certified Organization.

(5) Publicizing the name of the Certified Organization and content of the breach (*e.g.*, publicizing on the website of the Accountability Agent).

(6) If the breach of III Program Requirements constitutes a breach of *the Personal Data Protection Act*, the III shall report the name of the Certified Organization and the breach, to PEAs.

Q14: Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].

If the III reasonably believes that the breach of III Program Requirements by the Certified Organization constitutes a breach of *the Personal Data Protection Act*, the III has the power to report the name of the Certified Organization and the breach to the PEA. The PEA will be responsible for imposing punishment.

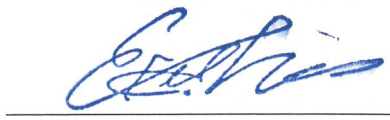
Q15: Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

1. If enforcement entities in APEC Economies make a request that reasonably relates to matters involving APEC, Accountability Agents and the CBPRs, the III will cooperate and provide necessary information.

2. Enforcement entities may send their requests to the III's email address (which will be provided on the website of the Accountability Agent). If necessary, the III may report such requests to PEAs.

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party attests to the truth of the answers given.



11.4.2022

[Signature of person who has authority to commit party to the agreement] **[Date]**

[Typed name]

CHENG HONG CHO, PH.D.

[Typed title]

PRESIDENT

[Typed name of organization]

INSTITUTE FOR INFORMATION INDUSTRY

[Address of organization]

For III's latest address, please see the following link:
https://web.iii.org.tw/SiteInfo/ContactUs.aspx?fm_sqno=48&ff_sqno=13

[Email address]

chc@iii.org.tw

[Telephone number]

+886-2- 6631-8899

APEC recognition is limited to one year from the date of recognition. Each year one month prior to the anniversary of the date of recognition, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.

ANNEXES

Annex 1	APEC CBPR Accountability Agent – Conflicts of Interest Policies and Procedures
Annex 2	III Program Requirements – CBPR: 2016
Annex 3	III Program Requirements – CBPR: 2021
Annex 4	Guideline for the Operation of Dispute Resolution Mechanism of the Domestic Certification System

ANNEX 1: APEC CBPR ACCOUNTABILITY AGENT – CONFLICTS OF INTEREST POLICIES AND PROCEDURES

THE CHINESE TEXT SHALL BE THE AUTHENTIC TEXT

INSTITUTE FOR INFORMATION INDUSTRY

SCIENCE AND TECHNOLOGY LAW INSTITUTE

APEC CBPR Accountability Agent – Conflicts of Interest Policies and Procedures

Controlled Document

Amendment History

Version	Effective Date	Reasons for Amendment
V1.0		

1. Purpose

The purpose of drafting the APEC CBPR Accountability Agent – Conflicts of Interest Policies and Management Procedures ('Conflicts of Interest Policies and Procedures') is to fairly perform all the tasks of an Accountability Agent of the Asian Pacific Economic Cooperation Cross Boarder Privacy Rules System ('APEC CBPRs').

The Conflicts of Interest Policies and Procedures are made subject to the following laws and regulations:

- the Conflicts of Interest Criteria (Criteria (1)-(3)) of the APEC Accountability Agent Recognition Criteria;
- Ethical Management in Operating Procedures of the Institute for Information Industry ('III');
- Article 24 of the Foundations Act;
- Guidelines for the Ethical Management in Operating Procedures of the Foundations Supervised by the Ministry of Economic Affairs.

2. Application and Scope

The scope of the Conflicts of Interest Policies and Procedures is to address conflicts of interest that arise from the performance of the following procedures:

- APEC CBPRs certifications;
- APEC CBPRs recertifications;
- mid-term audits;
- dispute resolution procedures.

3. Authorized Personnel

(1) Director General

The Director General is the person who performs the final review and is the final decision maker regarding whether there is a conflict of interest existing between an Applicant/ Participant Organization and the III, and what measures should be undertaken to avoid the conflict of interest.

(2) Director

The Director is the person who reviews whether there is a conflict of interest existing between the Applicant Organization/Participant Organization and the III, and what measures should be undertaken to avoid the conflict of interest.

(3) Executive Team

Members of the Executive Team are people who execute and implements the Conflicts of Interest Policies and Procedures, who determine whether there is a conflict of interest existing between the Applicant Organization/Participant Organization and the III and what measures should be undertaken to avoid the conflict of interest, and who keep records relating to this process.

4. Definition

4.1 Business Functions

Business Functions is defined as the III performing the following functions:

- APEC CBPRs certifications;
- APEC CBPRs recertifications;
- mid-term audits;
- dispute resolution procedures.

4.2 Executive Personnel

Executive Personnel means employees or dispatched workers of the III who performs the Business Functions.

4.3 Executive Team

Executive Team means the team within the III that performs the Business Functions.

4.4 Applicant/ Participant Organization

Applicant/Participant Organization means the organization that:

- applies for an APEC CBPRs certification;
- applies for an APEC CBPRs recertification;
- applies for a mid-term audit;
- is subject to a complaint under the dispute resolution procedure.

4.5 Related Persons

Related Persons means:

- The spouse of an Executive Personnel or family members living together with the Executive Personnel;
- Relatives of the Executive Personnel who are second degree relatives by blood or by law.

4.6 Interests

Interests include property interests and non-property interests. Interests received or given occasionally in accordance with accepted social customs which do not adversely affect specific rights and obligations shall be excluded.

4.6.1 Property interests include:

(1) Movable property and real estate;

(2) Cash, deposits, foreign currencies, and securities;

(3) Obligatory rights or other property rights;

(4) Other interests with economic value or that can be acquired through money exchange.

4.6.2 Non-property interests mean the appointment, promotion, transfer, and other personnel measures of the Executive Personnel and Related Persons in the III or other entities.

4.7 Conflicts of Interest

Conflicts of interest may arise out of the following circumstances:

(1) The III and the Applicant/Participant Organization being under common control or supervision such that the Applicant/Participant Organization can exert undue influence on the III, and vice versa.

(2) There are significant monetary arrangements or commercial relationships between the Science and Technology Law Institute of the Institute for Information Industry (‘STLI’) and the Applicant/Participant Organization, which are outside of the fee charged for certification and participation in the APEC CBPRs, or the relationship between the STLI and the Applicant/Participant Organization is one that may compromise the III’s ability to render a fair decision with respect to such an Applicant/Participant Organization.

(3) In regards to departments other than the STLI within the III (‘Other III Departments’), there are significant monetary arrangements or commercial relationships between Other III Departments and the Applicant/Participant Organization, which are outside of the fee

charged for certification and participation in the APEC CBPR System, or the relationship between Other III Departments and the Applicant/Participant Organization is one that may compromise the III's ability to render a fair decision with respect to such an Applicant/Participant Organization.

(4) Directors and supervisors of the III are employed by the Applicant/Participant Organization, or serving as directors in a voting capacity on the board of directors of the Applicant/Participant Organization.

(5) The officer of the III who supervises the Executive Team serves as a director in a voting capacity on the board of directors of the Applicant/Participant Organization.

(6) The Executive Personnel and Related Persons serve as directors in a voting capacity on the board of directors of the Applicant/Participant Organization, or are owners or persons responsible for the management of the Applicant/Participant Organization, or actively or passively obtain any unjust enrichment while performing the Business Functions.

5. Procedures regarding the Management of the Avoidance of Conflicts of Interest

5.1 Disclosure of Conflicts of Interest

Any Executive Personnel must complete the *Executive Personnel Conflicts of Interest Disclosure Form* prior to accepting any application lodged by the Applicant/Participant Organization. The Applicant/Participant Organization must complete the *Applicant/Participant Organization Conflicts of Interest Statement*, disclosing whether there are conflicts of interest and the circumstances regarding the conflict.

5.1.1 Disclosure of Conflicts of Interest – Executive Personnel

The Executive Personnel must disclose the following in the *Executive Personnel Conflicts of Interest Disclosure Form*:

(1) whether the Executive Personnel serves as a director in a voting capacity on the board of directors of the Applicant/Participant Organization;

(2) whether the Executive Personnel and Related Persons are the owner or the person responsible for the management of the Applicant/Participant Organization;

(3) whether the Executive Personnel and Related Persons would obtain any Property Interests and Non-Property Interests while performing the Business Functions regarding this particular application.

5.1.2 Disclosure of Conflicts of Interest – Applicant/Participant Organization

The Applicant/Participant Organization must disclose the following in the *Applicant/Participant Organization Conflicts of Interest Statement*:

(1) whether the Applicant/Participant Organization and the III is being under common control or supervision such that the Applicant/Participant Organization can exert undue influence on the III, and vice versa;

(2) whether there are significant monetary arrangements or commercial relationships between the III and the Applicant/Participant Organization, which are outside of the fee charged for certification and participation in the APEC CBPR System, or whether the relationship between the III and the Applicant/Participant Organization is one that may compromise the III's ability to render a fair decision with respect to such an Applicant/Participant Organization;

(3) whether the directors and supervisors of the III are employed by the Applicant/Participant Organization and whether the directors and supervisors are serving as directors in a voting capacity on the board of directors of the Applicant/Participant Organization;

(4) whether the officer of the III who supervises the Executive Team serves as a director in a voting capacity on the board of directors of the Applicant/Participant Organization.

5.2 Determination of Conflicts of Interest and Measures to Avoid Conflicts of Interest

Prior to accepting the application, the Executive Team should determine whether there are conflicts of interest and decide what relevant measures should be taken. Such determination should be made by assessing the circumstances disclosed in the *Executive Personnel Conflicts of Interest Disclosure Form* and the *Applicant/Participant Organization Conflicts of Interest Statement*, along with the following principles:

(1) The Executive Team may accept the application, if it determines that there are no conflicts of interest;

(2) The Executive Team must reject the application or cease the dispute resolution procedure, if it determines that there are conflicts of interest arising out of the following circumstances:

- the Applicant/Participant Organization and the III is being under common control or supervision such that the Applicant/Participant Organization can exert undue influence on the III, and vice versa;

- there are significant monetary arrangements or commercial relationships between the STLI and the Applicant/Participant Organization, which are outside of the fee charged for certification and participation in the APEC CBPR System, or the relationship between the STLI and the Applicant/Participant Organization is one that may compromise III's ability to render a fair decision with respect to such an Applicant/Participant Organization.

(3) Relevant persons must cease to participate in the following arrangements, relationships, and positions, if the Executive Team determines there are conflicts of interest arising out of the following circumstances:

- significant monetary arrangements or commercial relationships between the III and the Applicant/Participant Organization, which are outside of the fee charged for certification and participation in the APEC CBPR System, or the relationship between the III and the Applicant/Participant Organization is one that may compromise III's ability to render a fair decision with respect to such an Applicant/Participant Organization;
- directors and supervisors of the III being employed by the Applicant/Participant Organization, or are serving as directors in a voting capacity on the board of directors of the Applicant/Participant Organization;
- the officer of the III who supervises the Executive Team serves as directors in a voting capacity on the board of directors of the Applicant/Participant Organization;
- the Executive Personnel and Related Persons serve as directors in a voting capacity on the board of directors of the Applicant/Participant Organization, or are the owner or the person responsible for the management of the Applicant/Participant Organization, or actively or passively obtain any unjust enrichment while performing the Business Functions.

(4) After the Executive Team has made a determination according to 5.2, the determination must be reviewed by the Director. The Director General of the Science and Technology Institute of the Institute for Information Industry must perform the final review and make the final decision regarding the determination. If the Director General of the Science and Technology Institute of the Institute for Information Industry has a conflict of interest, the supervising officer of the Executive Team should perform the final review and make the final decision regarding the determination.

5.3 Records and Audit

5.3.1 Record Keeping

The Executive Team must keep a record regarding any persons who have a final decision made against them under 5.2 - that there exists a conflict of interest and that they should take measures to avoid such conflicts of interest.

5.3.2 Report

The STLI should publish annual reports regarding how the III reviews and performs the Conflicts of Interest Policies and Procedures. Conflicts of interest management projects should be created and delivered annually. This is for the purpose of recording the decision

making process of the III when performing its duties under the Conflicts of Interest Policies and Procedures, and fulfilling its reporting duties as an Accountability Agent of the APEC CBPRs.

5.3.3 Audit

The annual report reviewing the implementation of the Conflicts of Interest Policies and Procedures should be included in an annual quality audit project for the purpose of inspecting whether the III has effectively implemented the Conflicts of Interest Policies and Procedures.

6. Effect of Breach

Any employee of the III who breaches the Conflicts of Interest Policies and Procedures may be subject to punishment and liability according to the Working Rules of the III, the Ethical Management in Operating Procedures of the III and the terms and condition of his or her Employment Service Agreement.

7. Documents and Flow Charts

Document	Document No	Records Kept Until
Appendix 1: Conflicts of Interest Criteria	N/A	Permanent
Appendix 2: Conflicts of Interest Procedure Chart	N/A	Permanent
Appendix 3: Executive Personnel Conflicts of Interest Disclosure Form	N/A	Permanent
Appendix 4: Applicant/Participant Organization Conflicts of Interest Statement	N/A	Permanent
Appendix 5: Conflicts of Interest – Determination Form	N/A	Permanent

ANNEX 2: III PROGRAM REQUIREMENTS – CBPR: 2016

Appendix 1: APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS MAP

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant organization's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* ('PDPA')
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: ● Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). ● Is in accordance with the principles of the APEC	**FDCR r 4.2 Personal Information Protection and Administration policies** An organization shall formulate the basis, purpose, and basic responsibility of maintenance and management of personal information in writing and disclose the abovementioned information to the personnel. **FDCR r 4.5.1.1 Collection**

statements and/or hyperlinks to the same.	Privacy Framework; ● Is easy to find and accessible. ● Applies to all personal information; whether collected online or offline. ● States an effective date of Privacy Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs. **FDCR r 4.5.1.6 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements: (1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner.

		(3) Provide the cause for exemption from notification and way of confirmation. **FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **Article 8, Paragraph 1 of PDPA** A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: 1. the name of the government or non-government agency; 2. the purpose of the collection; 3. the categories of the personal data to be collected;

		4. the time period, territory, recipients, and methods of which the personal data is used; 5. the data subject's rights under Article 3 and the methods for exercising such rights; and 6. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. **Article 9, Paragraph 1 of PDPA** A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19 which was not provided by the data subject, inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of the preceding article.
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: ● The statement describes the collection practices and policies applied to all covered personal information	Same as above.

	collected by the Applicant. ● the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and ● The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes	Same as above.

	for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability	Same as above.

	Agent must verify whether the applicable qualification is justified.	
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a **functional** e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	Same as above.
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability	Same as above.

	Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: ● The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). ● The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the	Same as above.

	Accountability Agent must verify whether the applicable qualification is justified.	
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	**FDCR r 4.5.1.1 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs. **FDCR r 4.5.1.6 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements:

		(1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. **Article 8, Paragraph 1 of PDPA** A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: 1. the name of the government or non-government agency; 2. the purpose of the collection; 3. the categories of the personal data to be collected; 4. the time period, territory, recipients, and methods of which the personal data is used;

		5. the data subject's rights under Article 3 and the methods for exercising such rights; and 6. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. **Article 9, Paragraph 1 of PDPA** A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19 which was not provided by the data subject, inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of the preceding article.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's	Same as above

behalf), do you indicate the purpose(s) for which personal information is being collected?	website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the	**FDCR r 4.5.1.1 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations.

	Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	(3) Keep records of matters specified in the preceding two paragraphs. **FDCR r 4.5.1.6 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements: (1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. **Article 8, Paragraph 1 of PDPA**

		A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: 1. the name of the government or non-government agency; 2. the purpose of the collection; 3. the categories of the personal data to be collected; 4. the time period, territory, recipients, and methods of which the personal data is used; 5. the data subject's rights under Article 3 and the methods for exercising such rights; and 6. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. **Article 9, Paragraph 1 of PDPA** A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19 which was not provided by the data subject,

		inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of the preceding article.

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* ('PDPA')
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	**FDCR r 4.4.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of personal information management system ('PIMS'), and compile and maintain the list of personal information files and related procedures. **FDCR r 4.5.1 Basic Principles**

		An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith and within the minimum scope of specific purpose and in accordance with the purpose of collection.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: ● Each type of data collected ● The corresponding stated purpose of collection for each; and ● All uses that apply to each type of data ● An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection	**FDCR r 4.5.1 Basic Principles** An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith and within the minimum scope of specific purpose and in accordance with the purpose of collection. **FDCR r 4.5.1.1 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws.

	Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	(2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs. **Article 5 of PDPA** The collection, processing and use of personal data shall be carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, shall not exceed the necessary scope of specific purposes, and shall have legitimate and reasonable connections with the purposes of collection. **Article 15 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases:

		1. where it is within the necessary scope to perform its statutory duties; 2. where consent has been given by the data subject; or 3. where the rights and interests of the data subject will not be infringed upon. **Article 19, Paragraph 1 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases: 1. where it is expressly required by law; 2. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data;

		3. where the personal data has been disclosed to the public by the data subject or has been made public lawfully; 4. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject; 5. where consent has been given by the data subject; 6. where it is necessary for furthering public interest; 7. where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or 8. where the rights and interests of the data subject will not be infringed upon.
7. Do you collect personal information (whether directly or through the use of third parties acting on	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information	**FDCR r 4.4.1 Applicable acts and related regulations** An organization shall identify the applicable acts and explicitly reveal the consistency between the internal PIMS and related domestic personal information protection laws in terms of content

your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	and implementation. An organization shall also adjust the internal PIMS according to changes in applicable laws and regulations. **FDCR r 4.5.1 Basic Principles** An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith and within the minimum scope of specific purpose and in accordance with the purpose of collection. **FDCR r 4.5.1.1 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations.

		(3) Keep records of matters specified in the preceding two paragraphs. The collection, processing and use of personal data shall be carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, shall not exceed the necessary scope of specific purposes, and shall have legitimate and reasonable connections with the purposes of collection. **Article 15 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases: 1. where it is within the necessary scope to perform its statutory duties; 2. where consent has been given by the data subject; or

		3. where the rights and interests of the data subject will not be infringed upon. **Article 19, Paragraph 1 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases: 1. where it is expressly required by law; 2. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data; 3. where the personal data has been disclosed to the public by the data subject or has been made public lawfully; 4. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as

		disclosed by the data collector, may not lead to the identification of a specific data subject; 5. where consent has been given by the data subject; 6. where it is necessary for furthering public interest; 7. where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or 8. where the rights and interests of the data subject will not be infringed upon.

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* (‘PDPA’)
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant’s Privacy Statement(s) in	**FDCR r 4.5.1 Basic Principles** An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith and within the minimum scope of specific purpose and in accordance with the purpose of collection.

provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	**FDCR r 4.5.1.2 Processing** To create or use personal information files, an organization shall meet the following requirements for record, import, saving, editing, modification, reproduction, retrieval, deletion, export, connection, and internal transmission of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Formulate proper and legal procedures of deletion and destruction of personal information. (4) Keep records of matters specified in the preceding three paragraphs. **FDCR r 4.5.1.3 Use** An organization shall meet the following requirements for use of personal information:

		(1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: ● Online at point of collection	**FDCR r 4.5.1.3 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **Article 16 of PDPA**

	● Via e-mail ● Via preference/profile page ● Via telephone ● Via postal mail, or ● Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or	Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests;

	related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification45 of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests.
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure	**FDCR r 4.4.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of PIMS, and compile and maintain the list of personal information files and related procedures.

information controllers? If YES, describe.	and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1） each type of data disclosed or transferred; 2） the corresponding stated purpose of collection for each type of disclosed data; and 3） the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or	**FDCR r 4.5.1.3 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs.
11. Do you transfer personal information to personal information processors? If YES, describe.		**FDCR r 4.4.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of PIMS, and compile and maintain the list of personal information files and related procedures. **FDCR r 4.5.1.3 Use**

	related purposes.	An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee.

		(2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the

		instruction given by the principal a breach of the System or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.		**FDCR r 4.4.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of PIMS, and compile and maintain the list of personal information files and related procedures. **FDCR r 4.5.1.3 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws.

		(3) Keep records of matters specified in the preceding two paragraphs. **FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained.

		(5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the System or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes.	**FDCR r 4.5.1.3 Use** An organization shall meet the following requirements for use of personal information:

take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: ● Online at point of collection ● Via e-mail ● Via preference/profile page ● Via telephone ● Via postal mail, or ● Other (in case, specify) Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the	(1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information.

	individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	(3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the System or applicable laws, the trustee shall inform the principal immediately.

		The principal shall confirm the performance of the trustee on a regular basis and keep related records. **Article 16 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law;

		2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests.

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* ('PDPA')
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: ● Online at point of collection ● Via e-mail ● Via preference/profile page	**FDCR r 4.5.1.1 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations.

	● Via telephone ● Via postal mail, or ● Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	(3) Keep records of matters specified in the preceding two paragraphs. **Article 15 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases: 1. where it is within the necessary scope to perform its statutory duties; 2. where consent has been given by the data subject; or 3. where the rights and interests of the data subject will not be infringed upon. **Article 19, Paragraph 1 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases:

		1. where it is expressly required by law; 2. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data; 3. where the personal data has been disclosed to the public by the data subject or has been made public lawfully; 4. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject; 5. where consent has been given by the data subject; 6. where it is necessary for furthering public interest; 7. where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or 8. where the rights and interests of the data subject will not be infringed upon.

		FDCR r 4.5.1.6 Performance of notification For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements: (1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. (4) Keep records of matters specified in the preceding three paragraphs. **FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection,

		termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so	**FDCR r 4.5.1.3 Use** An organization shall meet the following requirements for use of personal information:

choice in relation to the use of their personal information? Where YES describe such mechanisms below.	that they may exercise choice in relation to the use of their personal information, such as: ● Online at point of collection ● Via e-mail ● Via preference/profile page ● Via telephone ● Via postal mail, or ● Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to	(1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **Article 16 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA**

	exercise choice may be provided to the individual after collection, but before: ● being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and ● Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for	Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests.

	individuals to exercise choice in relation to the use of their personal information must be provided.	**FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.

16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: ● Online at point of collection ● Via e-mail ● Via preference/profile page ● Via telephone ● Via postal mail, or ● Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be	**FDCR r 4.5.1.3 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **Article 16 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021

	provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: ● disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified.	**Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject;

	Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests. **FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply.

		(3) Keep records of matters specified in the preceding two paragraphs.
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	**FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.2 Procedures of exercise of rights** An organization shall at least meet the following requirements for procedures of requests made by parties in accordance with Article 4.5.2.1: (1) Have the way to allow parties to make requests. (2) Have the way to confirm the party's identity. (3) Have a way to confirm whether an organization may reject the exercise of rights of parties in accordance with applicable laws.

		(4) Have the way and contact to allow parties to raise complaints against the rejection of request or any dispute. **FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
18. When choices are provided to the individual offering the ability to limit the collection (question	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable.	**FDCR r 4.5.1.6 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of

14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	notification and confirmation, which shall at least meet the following requirements: (1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. (4) Keep records of matters specified in the preceding three paragraphs. **FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.2 Procedures of exercise of rights**

		An organization shall at least meet the following requirements for procedures of requests made by parties in accordance with Article 4.5.2.1: (1) Have the way to allow parties to make requests. (2) Have the way to confirm the party's identity. (3) Have a way to confirm whether an organization may reject the exercise of rights of parties in accordance with applicable laws. (4) Have the way and contact to allow parties to raise complaints against the rejection of request or any dispute. **FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and

		consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	**FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and

		consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure	**FDCR r 4.5.1 Basic Principles** An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith and within the minimum scope of specific purpose and in accordance with the purpose of collection. **FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.5 Complaints and consultation**

	that choices, when offered, can be honored, must be provided.	An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* ('PDPA')
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify	**FDCR r 4.5.3.1 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing. (2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.

	and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for	**FDCR r 4.5.2.4 Procedures of supplement, correction, deletion, termination of collection, processing and use of personal information** An organization shall meet the following requirements for supplement, correction, deletion, termination of collection, processing, and use of personal information upon request of parties: (1) Make a decision within 30 days. (2) Notify the party of decision in writing, with the reason for refusal attached if applicable. (3) Notify the party of 30-day extension of decision making, with the reason attached. (4) Keep records of matters specified in the preceding three paragraphs.

	the purposes of use, are required for compliance with this principle.	**FDCR r 4.5.3.1 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing. (2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure	**FDCR r 4.5.3.1 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing.

information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	(2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed.	**FDCR r 4.5.3.1 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing.

the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.	The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	(2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated.	**FDCR r 4.5.3.1 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing. (2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information.

	The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	(4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization. **FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained.

		(5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the FDCR or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* ('PDPA')
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	**FDCR r 4.5.3.2 Security management measures** For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of personal information. The abovementioned safety management measures shall at least include: (1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety).

		(3) Technical safety management measures (such as information transmission and system monitoring). **FDCR r 7.1.1 Documents** An organization shall compile and keep the following documents: (1) Personal information protection and administration policy. (2) Personal information protection and management manual and related specific rules. (3) Forms related to the personal information internal management procedures.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use,	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: ● Authentication and access control (eg password protections)	**FDCR r 4.5.3.2 Security management measures** For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of personal information. The abovementioned safety management measures shall at least include:

modification or disclosure of information or other misuses?	● Encryption ● Boundary protection (eg firewalls, intrusion detection) ● Audit logging ● Monitoring (eg external and internal audits, vulnerability scans) ● Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.	(1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety). (3) Technical safety management measures (such as information transmission and system monitoring).

	Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	
28. Describe how the safeguards you identified in response to question 27 are	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must	**FDCR r 4.4.3 Risk control measures**

proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	An organization shall identify potential risks that it may face when collecting, processing or using personal information within the scope of PIMS and formulate management and control measures if necessary. **FDCR r 4.5.3.2 Security management measures** For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of personal information. The abovementioned safety management measures shall at least include: (1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety). (3) Technical safety management measures (such as information transmission and system monitoring).

29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: ● Training program for employees ● Regular staff meetings or other communications ● Security policy signed by employees ● Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	**FDCR r 4.2 Personal Information Protection and Administration policies** An organization shall formulate the basis, purpose, and basic responsibility of maintenance and management of personal information in writing and disclose the abovementioned information to the personnel. **FDCR r 4.5.3.3 Supervision of personnel** An organization shall take necessary and proper monitoring measures for collection, processing, and use of personal information. **FDCR r 4.6.1 General requirements** An organization shall appropriately ensure that the personnel has the correct knowledge and capability of personal information management.

		FDCR r 4.6.2 Basic training An organization shall provide necessary training programs regarding the personal information management for the personnel. **FDCR r 4.6.3 Training for authorized personnel** An organization shall determine the necessary capabilities of the authorized personnel related to the PIMS and plan the implement the training programs subject to demands. **FDCR r 4.6.4 Record and improvement** An organization shall keep records and set up improvement mechanisms for training programs provided for the personnel.
30. Have you implemented safeguards that are proportional to the likelihood and severity of	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards.	**FDCR r 4.4.3 Risk control measures** An organization shall identify potential risks that it may face when collecting, processing or using personal information within

the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?	The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	the scope of PIMS and formulate management and control measures if necessary. **FDCR r 4.4.4 Resource management** An organization shall provide and maintain human resources and software and hardware required in the PIMS, ensure the effective implementation, maintenance, and improvement of resource management, and keep records of resource management. **FDCR r 4.5.3.2 Security management measures** For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of personal information. The abovementioned safety management measures shall at least include:

30.d) Physical security?		(1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety). (3) Technical safety management measures (such as information transmission and system monitoring). **FDCR r 4.5.3.3 Supervision of personnel** An organization shall take necessary and proper monitoring measures for collection, processing, and use of personal information. **FDCR r 4.6.1 General requirements** An organization shall appropriately ensure that the personnel has the correct knowledge and capability of personal information management.

		FDCR r 4.6.2 Basic training An organization shall provide necessary training programs regarding the personal information management for the personnel. **FDCR r 4.6.3 Training for authorized personnel** An organization shall determine the necessary capabilities of the authorized personnel related to the PIMS and plan the implement the training programs subject to demands. **FDCR r 4.6.4 Record and improvement** An organization shall keep records and set up improvement mechanisms for training programs provided for the personnel.
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information.	**FDCR r 4.5.1.2 Processing** To create or use personal information files, an organization shall meet the following requirements for record, import, saving,

	Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	editing, modification, reproduction, retrieval, deletion, export, connection, and internal transmission of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Formulate proper and legal procedures of deletion and destruction of personal information. (4) Keep records of matters specified in the preceding three paragraphs. **FDCR r 4.5.3.2 Security management measures** For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of

		personal information. The abovementioned safety management measures shall at least include: (1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety). (3) Technical safety management measures (such as information transmission and system monitoring).
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	**FDCR r 4.4.6 Emergency response** To avoid potential disadvantages and impacts arising from accidents, an organization shall formulate the emergency response measures, which shall at least include: (1) Proper notification upon investigation and provision of channels for subsequent queries and processing. (2) Measures that prevent the damage from expanding. (3) Measures that prevent the occurrence of similar accidents.

		(4) Submission of the report on the accident to the grant authority. **FDCR r 4.5.3.2 Security management measures** For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of personal information. The abovementioned safety management measures shall at least include: (1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety). (3) Technical safety management measures (such as information transmission and system monitoring).
33. Do you have processes in place to test the	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant	**FDCR r 6. Effectiveness measurement**

effectiveness of the safeguards referred to above in question 32? Describe below.	adjusts their security safeguards to reflect the results of these tests.	An organization shall establish a set of analysis mechanisms for the implementation of PIMS, which allow the management representative to determine whether the procedures and mechanisms set up in the PIMS are effective, and keep related records in order to ensure the effective operation of the system. **FDCR r 9.1 Regular Review** To implement the personal information protection and management, the personal information management representative shall convene the review meeting every year on a regular basis to review the PIMS, compile the written report, and report the related resolutions to the top management. The regularly held review meeting shall review the following and compile a review report: (1) Implementation and analysis of PIMS. (2) Effect of corrective and preventive actions. (3) Result of effectiveness measurement.

		(4) Amendments to applicable laws and regulations related to the processing of personal information. When determining the adjustment in the PIMS, the top management shall take the following into account and make adjustments accordingly: (1) The review report. (2) Changes in social situation, public awareness, and technological development. (3) Changes in the scope of business. (4) Internal and external recommendations for improvements. (5) Changes that may affect the PIMS.
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify	**FDCR r 4.4.3 Risk control measures** An organization shall identify potential risks that it may face when collecting, processing or using personal information within the scope of PIMS and formulate management and control measures if necessary.

	whether recommendations made in the audits are implemented.	**FDCR r 8. Internal Evaluation** An organization shall carry out the annual internal evaluation in order to understand whether the PIMS complies with the following requirements: (1) Applicable laws and the FDCR. (2) Personal information protection and administration policy, manual, and related specific rules. An organization shall plan the way and procedures of internal evaluation in order to determine the principle, scope, frequency and method of internal evaluation. An organization shall compile the written report on the planning, implementation, reports, improvements, and follow-up of internal evaluation. An internal evaluation plan shall be planned by an internal auditor or verifier of the domestic certification system, who is responsible to ensure the effectiveness of internal evaluation and compile the internal evaluation report.

		FDCR r 9.1 Regular Review To implement the personal information protection and management, the personal information management representative shall convene the review meeting every year on a regular basis to review the PIMS, compile the written report, and report the related resolutions to the top management. The regularly held review meeting shall review the following and compile a review report: (1) Implementation and analysis of PIMS. (2) Effect of corrective and preventive actions. (3) Result of effectiveness measurement. (4) Amendments to applicable laws and regulations related to the processing of personal information. When determining the adjustment in the PIMS, the top management shall take the following into account and make adjustments accordingly: (1) The review report.

		(2) Changes in social situation, public awareness, and technological development. (3) Changes in the scope of business. (4) Internal and external recommendations for improvements. (5) Changes that may affect the PIMS. **FDCR r 9.2 Corrective and preventive actions** According to the result of internal evaluation and the implementation of the system, an organization shall plan the corrective and preventive actions and ensure the implementation of related actions. **FDCR r 9.2.1 Corrective actions** To direct against potential risk of incompliance, an organization shall plan and complete the corrective actions and the following:

		(1) Confirming the content of incompliance and determining the cause (2) Evaluating demands and proposing the corrective actions to ensure the absence of occurrence of incompliance. (3) Setting up a proper period for execution. (4) Recording the result of corrective actions. (5) Reviewing the result of corrective actions. **FDCR r 9.2.2 Preventive Corrections** For potential incompliance, an organization shall plan and complete the preventive actions and the following： (1) Confirm the content of potential incompliance and determine the cause based on the risks of possession of personal information that an organization may face. (2) Evaluate demands and propose the preventive actions to ensure the absence of occurrence of incompliance.

		(3) Set up a proper period for execution. (4) Record the result of corrective actions. (5) Review the result of preventive actions.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	**FDCR r 4.4.6 Emergency response** To avoid potential disadvantages and impacts arising from accidents, an organization shall formulate the emergency response measures, which shall at least include: (1) Proper notification upon investigation and provision of channels for subsequent queries and processing. (2) Measures that prevent the damage from expanding. (3) Measures that prevent the occurrence of similar accidents. (4) Submission of the report on the accident to the grant authority. **FDCR r 4.5.3.2 Security management measures**

sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of personal information. The abovementioned safety management measures shall at least include: (1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety). (3) Technical safety management measures (such as information transmission and system monitoring). **FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards

		and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission.

		(9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the FDCR or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* (‘PDPA’)

36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written	**FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.2 Procedures of exercise of rights** An organization shall at least meet the following requirements for procedures of requests made by parties in accordance with Article 4.5.2.1: (1) Have the way to allow parties to make requests. (2) Have the way to confirm the party's identity. (3) Have a way to confirm whether an organization may reject the exercise of rights of parties in accordance with applicable laws.

	procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(4) Have the way and contact to allow parties to raise complaints against the rejection of request or any dispute.
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where	**FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.2 Procedures of exercise of rights** An organization shall at least meet the following requirements for procedures of requests made by parties in accordance with Article 4.5.2.1: (1) Have the way to allow parties to make requests.

access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the	the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(2) Have the way to confirm the party's identity. (3) Have a way to confirm whether an organization may reject the exercise of rights of parties in accordance with applicable laws. (4) Have the way and contact to allow parties to raise complaints against the rejection of request or any dispute. **FDCR r 4.5.2.3 Inquiry, read, and copy** An organization shall meet the following requirements for inquiry, read, or copy of personal information upon request of parties: (1) Make a decision within 15 days. (2) Notify the party of decision in writing, with the reason for refusal attached if applicable. (3) Notify the party of 15-day extension of decision making, with the reason attached.

individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		(4) Keep records of matters specified in the preceding three paragraphs.
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e).	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner,	**FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.2 Procedures of exercise of rights**

38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an	operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	An organization shall at least meet the following requirements for procedures of requests made by parties in accordance with Article 4.5.2.1: (1) Have the way to allow parties to make requests. (2) Have the way to confirm the party's identity. (3) Have a way to confirm whether an organization may reject the exercise of rights of parties in accordance with applicable laws. (4) Have the way and contact to allow parties to raise complaints against the rejection of request or any dispute. **FDCR r 4.5.2.4 Procedures of supplement, correction, deletion, termination of collection, processing and use of personal information** An organization shall meet the following requirements for supplement, correction, deletion, termination of collection,

individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?		processing, and use of personal information upon request of parties: (1) Make a decision within 30 days. (2) Notify the party of decision in writing, with the reason for refusal attached if applicable. (3) Notify the party of 30-day extension of decision making, with the reason attached. (4) Keep records of matters specified in the preceding three paragraphs. **FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management

		representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** FDCR and the *Personal Data Protection Act* (‘PDPA’)

39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. ● Internal guidelines or policies (if applicable, describe how implemented) _____ ● Contracts _____ ● Compliance with applicable industry or sector laws and regulations ____ ● Compliance with self-regulatory applicant code and/or	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	**FDCR r 4.2 Personal Information Protection and Administration policies** An organization shall formulate the basis, purpose, and basic responsibility of maintenance and management of personal information in writing and disclose the abovementioned information to the personnel. **FDCR r 4.3 Personal information protection and administration manual** To establish a PIMS, an organization shall compile a personal information protection and administration manual specifying the rules and effective measures for the operations of the system. Specific rules shall at least include: (1) Applicable acts and related regulations. (2) Identification of all personal information kept by the enterprise. (3) Matters of collection, processing and use of personal information by the enterprise.

rules ____ ● Other (describe) ____		(4) Risk analysis and control measures related to personal information. (5) Emergency responses to accidents. (6) Authorization and responsibility of personal information management possessed by each department and level in an organization. (7) Exercise of rights of party. (8) Maintenance of correct personal information. (9) Safety management measures. (10) Supervision and rewards and punishments of personnel. (11) Supervision of commissioned collection, processing or use of personal information. (12) Training. (13) Management of documents and records related to PIMS. (14) Complaints and consultation. (15) Internal evaluation.

		(16) Corrective and preventive actions. (17) Regular review of the top management. **FDCR r 4.4.1 Applicable acts and related regulations** An organization shall identify the applicable acts and explicitly reveal the consistency between the internal PIMS and related domestic personal information protection laws in terms of content and implementation. An organization shall also adjust the internal PIMS according to changes in applicable laws and regulations. **FDCR r 9.1 Regular Review** To implement the personal information protection and management, the personal information management representative shall convene the review meeting every year on a regular basis to review the PIMS, compile the written report, and report the related resolutions to the top management.

		The regularly held review meeting shall review the following and compile a review report: (1) Implementation and analysis of PIMS. (2) Effect of corrective and preventive actions. (3) Result of effectiveness measurement. (4) Amendments to applicable laws and regulations related to the processing of personal information. When determining the adjustment in the PIMS, the top management shall take the following into account and make adjustments accordingly: (1) The review report. (2) Changes in social situation, public awareness, and technological development. (3) Changes in the scope of business. (4) Internal and external recommendations for improvements. (5) Changes that may affect the PIMS.

40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	**FDCR r 5.1 Top Management** The top management shall have the following responsibilities: (1) Determine the personal information protection and administration policy. (2) Determine the resource management. (3) Determine the organizational structure of personal information protection and management and responsibilities. (4) Review the management system on a regular basis. (5) Establish an effective communication mechanism. **FDCR r 5.2 Representative of top management** The top management shall assign one member to serve as the representative of personal information protection and management system, who shall have the following duties and responsibilities: (1) Maintain the effective operation of PIMS and establish a necessary personnel structure.

		(2) Ensure the impartiality and objectiveness of performance of duties. (3) Ensure the establishment, implementation, and maintenance of procedures required in the PIMS. (4) Report the implementation of and improvement mechanism for the PIMS to the top management. **FDCR r 5.3 Personal information administrator** An organization shall assign the personal information administrator that is equipped with one of the following qualifications to promote and ensure the effective operation of PIMS: (1) administrator of the domestic certification system. (2) internal auditor of the domestic certification system. (3) verifier of the domestic certification system.
41. Do you have procedures in place to receive, investigate and	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant	**FDCR r 4.5.2.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection,

respond to privacy-related complaints? Please describe.	has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1） A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2） A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3） A formal complaint-resolution process; AND/OR 4） Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation	termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **FDCR r 4.5.2.2 Procedures of exercise of rights** An organization shall at least meet the following requirements for procedures of requests made by parties in accordance with Article 4.5.2.1: (1) Have the way to allow parties to make requests. (2) Have the way to confirm the party's identity. (3) Have a way to confirm whether an organization may reject the exercise of rights of parties in accordance with applicable laws. (4) Have the way and contact to allow parties to raise complaints against the rejection of request or any dispute. **FDCR r 4.5.2.5 Complaints and consultation**

	of such procedures is required for compliance with this principle.	An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	**FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply.

		(3) Keep records of matters specified in the preceding two paragraphs.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	**FDCR r 4.5.2.5 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints.	**FDCR r 4.6.1 General requirements** An organization shall appropriately ensure that the personnel has the correct knowledge and capability of personal information management. **FDCR r 4.6.2 Basic training**

to privacy-related complaints? If YES, describe.	Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	An organization shall provide necessary training programs regarding the personal information management for the personnel. **FDCR r 4.6.3 Training for authorized personnel** An organization shall determine the necessary capabilities of the authorized personnel related to the PIMS and plan the implement the training programs subject to demands. **FDCR r 4.6.4 Record and improvement** An organization shall keep records and set up improvement mechanisms for training programs provided for the personnel.
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or	Where the Applicant answers **YES, the** Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal	**FDCR r 4.3 Personal information protection and administration manual** To establish a PIMS, an organization shall compile a personal information protection and administration manual specifying the rules and effective measures for the operations of the system. Specific rules shall at least include:

orders, including those that require the disclosure of personal information?	information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	(1) Applicable acts and related regulations. (2) Identification of all personal information kept by the enterprise. (3) Matters of collection, processing and use of personal information by the enterprise. (4) Risk analysis and control measures related to personal information. (5) Emergency responses to accidents. (6) Authorization and responsibility of personal information management possessed by each department and level in an organization. (7) Exercise of rights of party. (8) Maintenance of correct personal information. (9) Safety management measures. (10) Supervision and rewards and punishments of personnel. (11) Supervision of commissioned collection, processing or use of personal information.

		(12) Training. (13) Management of documents and records related to PIMS. (14) Complaints and consultation. (15) Internal evaluation. (16) Corrective and preventive actions. (17) Regular review of the top management. **FDCR r 4.4.1 Applicable acts and related regulations** An organization shall identify the applicable acts and explicitly reveal the consistency between the internal PIMS and related domestic personal information protection laws in terms of content and implementation. An organization shall also adjust the internal PIMS according to changes in applicable laws and regulations. **FDCR r 4.5.1.3 Use**

		An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **Article 16 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021

		Article 20, Paragraph 1 of PDPA Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or

		7. where it is for the data subject's rights and interests.
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? ● Internal guidelines or policies _____ ● Contracts _____ ● Compliance with applicable industry or sector laws and	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	**FDCR r 4.5.3.3 Supervision of personnel** An organization shall take necessary and proper monitoring measures for collection, processing, and use of personal information. **FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee.

regulations _____ ● Compliance with self-regulatory applicant code and/or rules _____ ● Other (describe) _____		(4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the FDCR or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.

47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: ● Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ ● Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	**FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal.

● Follow instructions provided by you relating to the manner in which your personal information must be handled? _____ ● Impose restrictions on subcontracting unless with your consent? _____ ● Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ ● Notify the Applicant in the case of a breach of the personal information		(7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the FDCR or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.

of the Applicant's customers? ● Other (describe) _____		
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	The Accountability Agent must verify the existence of such self-assessments.	**FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee.

		(4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the FDCR or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.

49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	**FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information. (3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal.

		(7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the FDCR or applicable laws, the trustee shall inform the principal immediately. The principal shall confirm the performance of the trustee on a regular basis and keep related records.
50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where	**FDCR r 4.5.3.2 Security management measures** For potential risks that an organization may face when collecting, processing and using personal information, an organization shall take necessary and proper safety management measures that prevent the leakage, loss, damage, tampering and infringement of personal information. The abovementioned safety management measures shall at least include:

described above is impractical or impossible?	the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	(1) Operating safety management measures (such as access control, technical review, identification, and media safety). (2) Physical safety management measures (such as physical and environmental safety). (3) Technical safety management measures (such as information transmission and system monitoring). **FDCR r 4.5.3.4 Supervision of commissioned collection, processing, or use of personal information** When commissioning others to collect, process, or use part or all of personal information, an organization shall formulate standards and monitoring measures for the appointed trustee and confirm the following: (1) Rights and obligations of the principal and trustee. (2) Scope, type, specific purpose, and period of commissioned collection, processing or use of personal information.

		(3) Safety management measures for personal information taken by the trustee. (4) Multiple trustees and scope of commission; the consent of the principal shall be obtained. (5) Report on the disposal of personal information and reporting cycle to the principal. (6) Personal information to be kept in accordance with the instruction given by the principal. (7) Instant report and remedies for accidents to the principal. (8) Return of personal information carriers and deletion of personal information possessed by the trustee upon termination or rescission of commission. (9) The trustee may only collect, process or use personal information within the scope designated by the principal. If the trustee considers the instruction given by the principal a breach of the FDCR or applicable laws, the trustee shall inform the principal immediately.

		The principal shall confirm the performance of the trustee on a regular basis and keep related records.

ANNEX 3: III PROGRAM REQUIREMENTS – CBPR: 2021

Appendix 1: APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS MAP

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant organization's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* ('PDPA')
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: ● Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be	**NDCR r 5.2 Personal Information Protection and Administration policies** Top management shall establish a personal information management policy that: (1) addresses relevant laws and regulations. (2) includes the purpose and objective of establishing a PIMS ('PIMS'). (3) includes a commitment to continue to improve the PIMS. The PIMS policy shall:

applicable privacy statements and/or hyperlinks to the same.	specified). ● Is in accordance with the principles of the APEC Privacy Framework; ● Is easy to find and accessible. ● Applies to all personal information; whether collected online or offline. ● States an effective date of Privacy Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(1) be in writing. (2) be communicated within the organization. **NDCR r 8.4.2 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs. **NDCR r 8.4.8 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements:

		(1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. **NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **Article 8, Paragraph 1 of PDPA** A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: 1. the name of the government or non-government agency;

		2. the purpose of the collection; 3. the categories of the personal data to be collected; 4. the time period, territory, recipients, and methods of which the personal data is used; 5. the data subject's rights under Article 3 and the methods for exercising such rights; and 6. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. **Article 9, Paragraph 1 of PDPA** A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19 which was not provided by the data subject, inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of the preceding article.
1.a) Does this privacy statement describe how	If **YES**, the Accountability Agent must verify that:	Same as above.

personal information is collected?	● The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. ● the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and ● The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	
1.b) Does this privacy statement describe the purpose(s) for which	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals of the	Same as above.

personal information is collected?	purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the	Same as above.

	purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a **functional** e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle.	Same as above.

collection? Where YES describe.	Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	Same as above.

1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: ● The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). ● The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability	Same as above.

	Agent must verify whether the applicable qualification is justified.	
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	**NDCR r 8.4.2 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs. **NDCR r 8.4.8 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements:

		(1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. **Article 8, Paragraph 1 of PDPA** A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: 1. the name of the government or non-government agency; 2. the purpose of the collection; 3. the categories of the personal data to be collected; 4. the time period, territory, recipients, and methods of which the personal data is used;

		5. the data subject's rights under Article 3 and the methods for exercising such rights; and 6. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. **Article 9, Paragraph 1 of PDPA** A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19 which was not provided by the data subject, inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of the preceding article.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website	Same as above

indicate the purpose(s) for which personal information is being collected?	link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes.	**NDCR r 8.4.2 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws.

be shared with third parties?	Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	(2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs. **NDCR r 8.4.8 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements: (1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. **Article 8, Paragraph 1 of PDPA**

		A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: 1. the name of the government or non-government agency; 2. the purpose of the collection; 3. the categories of the personal data to be collected; 4. the time period, territory, recipients, and methods of which the personal data is used; 5. the data subject's rights under Article 3 and the methods for exercising such rights; and 6. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. **Article 9, Paragraph 1 of PDPA** A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19 which was not provided by the data subject, inform the data subject of its source of data and

		other information specified in Subparagraphs 1 to 5, Paragraph 1 of the preceding article.

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* ('PDPA')
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf?	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard.	**NDCR r 8.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of personal information management system ('PIMS'), and compile and maintain the list of personal information files and related procedures. **NDCR r 8.4.1 General Principle**

5.c) Other. If YES, describe.	There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith, within the minimum scope of the specific purpose, and in accordance with the purpose of collection.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: ● Each type of data collected ● The corresponding stated purpose of collection for each; and ● All uses that apply to each type of data ● An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection	**NDCR r 8.4.1 General Principle** An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith, within the minimum scope of the specific purpose, and in accordance with the purpose of collection. **NDCR r 8.4.2 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations.

	Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	(3) Keep records of matters specified in the preceding two paragraphs. **Article 5 of PDPA** The collection, processing and use of personal data shall be carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, shall not exceed the necessary scope of specific purposes, and shall have legitimate and reasonable connections with the purposes of collection. **Article 15 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases: 1. where it is within the necessary scope to perform its statutory duties; 2. where consent has been given by the data subject; or 3. where the rights and interests of the data subject will not be infringed upon.

		Article 19, Paragraph 1 of PDPA Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases: 1. where it is expressly required by law; 2. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data; 3. where the personal data has been disclosed to the public by the data subject or has been made public lawfully; 4. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject; 5. where consent has been given by the data subject; 6. where it is necessary for furthering public interest;

		7. where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or 8. where the rights and interests of the data subject will not be infringed upon.
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	**NDCR r 8.1 Applicable acts and related regulations** An organization shall identify the applicable acts and explicitly reveal the consistency between the internal PIMS and related domestic personal information protection laws in terms of content and implementation. An organization shall also adjust the internal PIMS according to changes in applicable laws and regulations. **NDCR r 8.4.1 General Principle** An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith, within the minimum scope of the specific purpose, and in accordance with the purpose of collection.

		NDCR r 8.4.2 Collection An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs. The collection, processing and use of personal data shall be carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, shall not exceed the necessary scope of specific purposes, and shall have legitimate and reasonable connections with the purposes of collection. **Article 15 of PDPA**

		Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases: 1. where it is within the necessary scope to perform its statutory duties; 2. where consent has been given by the data subject; or 3. where the rights and interests of the data subject will not be infringed upon. **Article 19, Paragraph 1 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases: 1. where it is expressly required by law; 2. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data; 3. where the personal data has been disclosed to the public by the data subject or has been made public lawfully;

		4. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject; 5. where consent has been given by the data subject; 6. where it is necessary for furthering public interest; 7. where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or 8. where the rights and interests of the data subject will not be infringed upon.

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* (‘PDPA’)
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant’s Privacy	**NDCR r 8.4.1 General Principle** An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith, within the minimum scope of the specific purpose, and in accordance with the purpose of collection.

provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	**NDCR r 8.4.3 Processing** To create or use personal information files, an organization shall meet the following requirements for record, import, saving, editing, modification, reproduction, retrieval, deletion, export, connection, and internal transmission of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Formulate proper and legal procedures of deletion and destruction of personal information. (4) Keep records of matters specified in the preceding three paragraphs. **NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information:

		(1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as:	**NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **Article 16 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of

	● Online at point of collection ● Via e-mail ● Via preference/profile page ● Via telephone ● Via postal mail, or ● Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law.	its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided

	Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification45 of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests.
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product	**NDCR r 8.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of PIMS, and compile and maintain the list of personal information files and related procedures. **NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information:

	requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 4） each type of data disclosed or transferred;	(1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs.
11. Do you transfer personal information to personal information processors? If YES, describe.	5） the corresponding stated purpose of collection for each type of disclosed data; and 6） the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	**NDCR r 8.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of PIMS, and compile and maintain the list of personal information files and related procedures. **NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection.

		(2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization** When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures.

		(5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information. (7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately.

		The organization shall conduct regular review on other organisations and keep records.
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.		**NDCR r 8.2 Scope of personal information management** An organization shall identify and maintain the personal information files and procedures of collection, processing, and use of personal information, define the scope of PIMS, and compile and maintain the list of personal information files and related procedures. **NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs.

		NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures.

		(6) ensure that other organizations regularly report to the organization of how it manages personal information. (7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.
13. If you answered NO to question 12 or if otherwise	Where applicant answers **NO** to question 13, the Applicant must clarify under what	**NDCR r 8.4.4 Use**

appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: ● Online at point of collection ● Via e-mail ● Via preference/profile page ● Via telephone ● Via postal mail, or ● Other (in case, specify)	An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization** When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification.

	Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement.	(3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information. (7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends.

	Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	(10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records. **Article 16 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of

		the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests.

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* ('PDPA')
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: ● Online at point of collection ● Via e-mail	**NDCR r 8.4.2 Collection** An organization shall meet the following requirements for collection of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations. (3) Keep records of matters specified in the preceding two paragraphs.

	● Via preference/profile page ● Via telephone ● Via postal mail, or ● Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	**Article 15 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases: 1. where it is within the necessary scope to perform its statutory duties; 2. where consent has been given by the data subject; or 3. where the rights and interests of the data subject will not be infringed upon. **Article 19, Paragraph 1 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases: 1. where it is expressly required by law;

		2. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data; 3. where the personal data has been disclosed to the public by the data subject or has been made public lawfully; 4. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject; 5. where consent has been given by the data subject; 6. where it is necessary for furthering public interest; 7. where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or 8. where the rights and interests of the data subject will not be infringed upon. **NDCR r 8.4.8 Performance of notification**

		For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements: (1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. (4) Keep records of matters specified in the preceding three paragraphs. **NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.3 Complaints and consultation**

		An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: ● Online at point of collection ● Via e-mail ● Via preference/profile page	**NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs.

	● Via telephone ● Via postal mail, or ● Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: ● being able to make use of the personal information, when the purposes of such use is not related or compatible to the	**Article 16 of PDPA** Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject;

	purpose for which the information was collected, and ● Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests. **NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation:

		(1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: ● Online at point of collection ● Via e-mail ● Via preference/profile page ● Via telephone ● Via postal mail, or	**NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs. **Article 16 of PDPA**

	● Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: ● disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the	Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others;

	Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests. **NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly.

		(2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	**NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r. 8.5.2 Procedures to exercise data subject rights** An organization shall have relevant procedures to ensure that data subject rights are exercised, and should at least include the following: (1) establish procedures which allow data subjects to exercise their rights. (2) establish mechanisms to affirm the identity of data subjects.

		(3) determine whether an request to exercise data subject rights may be refused according to law. (4) provide contact information, enabling data subjects to make a complaint in regards to disputes arising from the exercise of their rights. (5) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights within the statutory period. (6) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights. Upon refusal, provide reasons and give notice. (7) provide reasons and notice, if the organization decides to extend time to make a decision as to whether to grant or refuse to grant the data subject to exercise its rights. (8) retain records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation:

		(1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their	**NDCR r 8.4.8 Performance of notification** For matters that should be informed under Personal Information Protection Act, an organization shall establish procedures of notification and confirmation, which shall at least meet the following requirements: (1) Send the notification at a time that complies with related personal information protection acts. (2) Send a notification in a proper manner. (3) Provide the cause for exemption from notification and way of confirmation. (4) Keep records of matters specified in the preceding three paragraphs.

	personal information, must be clearly worded and easily understandable in order to comply with this principle.	**NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **r. 8.5.2 Procedures to exercise data subject rights** An organization shall have relevant procedures to ensure that data subject rights are exercised, and should at least include the following: (1) establish procedures which allow data subjects to exercise their rights. (2) establish mechanisms to affirm the identity of data subjects. (3) determine whether an request to exercise data subject rights may be refused according to law. (4) provide contact information, enabling data subjects to make a complaint in regards to disputes arising from the exercise of their rights. (5) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights within the statutory period.

		(6) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights. Upon refusal, provide reasons and give notice. (7) provide reasons and notice, if the organization decides to extend time to make a decision as to whether to grant or refuse to grant the data subject to exercise its rights. (8) retain records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.

19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	**NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
20. What mechanisms are in place so that choices,	Where the Applicant does have mechanisms in place, the Accountability Agent must require	**NDCR r 8.4.1 General Principle**

where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	An organization shall make sure that the collection, processing, use or international transmission of personal information will be carried out in a manner of good faith, within the minimum scope of the specific purpose, and in accordance with the purpose of collection. **NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal

		information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* ('PDPA')
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that	**NDCR r 8.6 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing. (2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.

	is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax,	**NDCR r 8.5.2 Procedures to exercise data subject rights** An organization shall have relevant procedures to ensure that data subject rights are exercised, and should at least include the following: (1) establish procedures which allow data subjects to exercise their rights. (2) establish mechanisms to affirm the identity of data subjects. (3) determine whether an request to exercise data subject rights may be refused according to law.

	through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	(4) provide contact information, enabling data subjects to make a complaint in regards to disputes arising from the exercise of their rights. (5) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights within the statutory period. (6) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights. Upon refusal, provide reasons and give notice. (7) provide reasons and notice, if the organization decides to extend time to make a decision as to whether to grant or refuse to grant the data subject to exercise its rights. (8) retain records. **NDCR r 8.6 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing.

		(2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are	**NDCR r 8.6 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing. (2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.

transferred? If YES, describe.	made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the	**NDCR r 8.6 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing. (2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information.

personal information was disclosed? If YES, describe.	Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	(4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization.
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being	**NDCR r 8.6 Maintenance of correct personal information** An organization shall meet the following requirements for maintenance of correct personal information: (1) Ensure the correctness of personal information remains unchanged in the processing. (2) Correct wrong personal information in a timely manner. (3) Examine the correctness of personal information. (4) Stipulate that the personnel shall notify the users of modified or supplementary personal information due to the cause that is attributable to the organization. **NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization**

	made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information.

		(7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* ('PDPA')
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	**NDCR r 8.7 Security Measures** An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures. (2) technical measures. **NDCR r 7.3.1.1 Documents** An organization shall compile and keep the following documents:

		(1) Personal information protection and administration policy. (2) Personal information protection and management manual and related specific rules. (3) Forms related to the personal information internal management procedures.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: ● Authentication and access control (eg password protections) ● Encryption ● Boundary protection (eg firewalls, intrusion detection) ● Audit logging	**NDCR r 8.7 Security Measures** An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures. (2) technical measures.

	● Monitoring (eg external and internal audits, vulnerability scans) ● Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.	

	The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	
28. Describe how the safeguards you identified in response to question 27	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information,	**NDCR r 6.3 Risk and Planning** When planning to establish a PIMS, the organization should:

are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	(1) consider external and internal issues. (2) consider needs and expectations of stakeholders. (3) consider relevant laws and regulations. (4) plan risk management principles and procedures. (5) identify risks and measures. The organization may adopt principles of privacy by design and default. **NDCR r 6.3.1 Risk Analysis** The organisation should establish risk analysis procedures which should include: (1) establish principles related to risk, including risk analysis and management principles. (2) ensure that each risk analysis conducted produces consistent, effective and comparative results. (3) identify risks and who is subjected to the risk.

		(4) analyse risks, including identifying the consequences, the likelihood of occurrence and the degree of the risk. (5) evaluate risks, including comparing the outcome of the analysis and determine the priority in which each risk is to be dealt with. (6) identify the impact the risk has on the organisation and data subjects. **NDCR r 6.3.2 Risk Management** The organization shall utilize the outcome of its risk analysis to determine appropriate measures to manage its risks, and shall comply with Annexure A. **NDCR r 8.7 Security Measures** An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures.

		(2) technical measures. **NDCR r 4.1 External and Internal Issues** The organisation shall determine external and internal issues that relate to the implementation of its PIMS and that could affect the effective operation of its PIMS. **NDCR r 4.2 Needs and expectations of Stakeholders** The organisation shall identify stakeholders to the PIMS and their needs and expectations.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include:	**NDCR r 5.2 Personal Information Protection and Administration policies** Top management shall establish a personal information management policy that: (1) addresses relevant laws and regulations. (2) includes the purpose and objective of establishing a PIMS.

	● Training program for employees ● Regular staff meetings or other communications ● Security policy signed by employees ● Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	(3) includes a commitment to continue to improve the PIMS. The PIMS policy shall: (1) be in writing (2) be communicated within the organization. **NDCR r 8.8 Supervision of personnel** An organization shall take necessary and proper monitoring measures for collection, processing, and use of personal information. **NDCR r 7.2.1 General Principle** An organization shall ensure that its personnel has adequate skills and knowledge in regards to its PIMS and reward system. **NDCR r 7.2.2 Basic training**

		An organization shall provide necessary training programs regarding the personal information management for the personnel. **NDCR r 7.2.3 Training for authorized personnel** An organization shall determine the necessary capabilities of the authorized personnel related to the PIMS and plan the implement the training programs subject to demands. **NDCR r 7.2.4 Record and improvement** An organization shall keep records and set up improvement mechanisms for training programs provided for the personnel. **NDCR r 7.4 Communication** An organization shall establish mechanisms to effectively communicate information to its personnel.
30. Have you implemented safeguards	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability	**NDCR r 6.3 Risk and Planning**

that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks,	Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	When planning to establish a PIMS, the organization should: (6) consider external and internal issues. (7) consider needs and expectations of stakeholders. (8) consider relevant laws and regulations. (9) plan risk management principles and procedures. (10) identify risks and measures. The organization may adopt principles of privacy by design and default. **NDCR r 6.3.1 Risk Analysis** The organisation should establish risk analysis procedures which should include: (7) establish principles related to risk, including risk analysis and management principles. (8) ensure that each risk analysis conducted produces consistent, effective and comparative results.

intrusions, or other security failures? 30.d) Physical security?		(9) identify risks and who is subjected to the risk. (10) analyse risks, including identifying the consequences, the likelihood of occurrence and the degree of the risk. (11) evaluate risks, including comparing the outcome of the analysis and determine the priority in which each risk is to be dealt with. (12) identify the impact the risk has on the organisation and data subjects. **NDCR r 6.3.2 Risk Management** The organization shall utilize the outcome of its risk analysis to determine appropriate measures to manage its risks, and shall comply with Annexure A. **NDCR r 7.1 Resources** An organization shall provide and maintain human resources and software and hardware required in the PIMS, ensure the effective implementation, maintenance, and improvement of resource management, and keep records of resource management.

		NDCR r 8.7 Security Measures An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures. (2) technical measures. **NDCR r 4.1 External and Internal Issues** The organisation shall determine external and internal issues that relate to the implementation of its PIMS and that could affect the effective operation of its PIMS. **NDCR r 4.2 Needs and expectations of Stakeholders**

		The organisation shall identify stakeholders to the PIMS and their needs and expectations. **NDCR r 8.8 Supervision of personnel** An organization shall take necessary and proper monitoring measures for collection, processing, and use of personal information. **NDCR r 7.2.1 General Principle** An organization shall ensure that its personnel has adequate skills and knowledge in regards to its PIMS and reward system. **NDCR r 7.2.2 Basic training** An organization shall provide necessary training programs regarding the personal information management for the personnel. **NDCR r 7.2.3 Training for authorized personnel**

		An organization shall determine the necessary capabilities of the authorized personnel related to the PIMS and plan the implement the training programs subject to demands. **NDCR r 7.2.4 Record and improvement** An organization shall keep records and set up improvement mechanisms for training programs provided for the personnel.
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	**NDCR r 8.4.3 Processing** To create or use personal information files, an organization shall meet the following requirements for record, import, saving, editing, modification, reproduction, retrieval, deletion, export, connection, and internal transmission of personal information: (1) Have a specific purpose of collection that complies with the applicable laws. (2) Perform the obligations to collect personal information stipulated in other related regulations.

		(3) Formulate proper and legal procedures of deletion and destruction of personal information. (4) Keep records of matters specified in the preceding three paragraphs. **NDCR r 8.7 Security Measures** An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures. (2) technical measures.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the	**NDCR r 8.10 Emergency response** To avoid potential disadvantages and impacts arising from accidents, an organization shall formulate the emergency response measures, which shall at least include: (1) Proper notification upon investigation and provision of channels for subsequent queries and processing.

	Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	(2) Measures that prevent the damage from expanding. (3) Measures that prevent the occurrence of similar accidents. (4) Submission of the report on the accident to the grant authority. **NDCR r 8.7 Security Measures** An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures. (2) technical measures.
33. Do you have processes in place to test the effectiveness of the safeguards referred to	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	**NDCR r 9.1 Effectiveness measurement** An organization shall establish a set of analysis mechanisms for the implementation of PIMS, which allow the management representative to determine whether the procedures and mechanisms set up in the PIMS are

above in question 32? Describe below.		effective, and keep related records in order to ensure the effective operation of the system. **NDCR r 9.3 Regular Review** To implement the personal information protection and management, the personal information management representative shall convene the review meeting every year on a regular basis to review the PIMS, compile the written report, and report the related resolutions to the top management. The regularly held review meeting shall review the following and compile a review report: (1) Implementation and analysis of PIMS. (2) Effect of corrective and preventive actions. (3) Result of effectiveness measurement. (4) Amendments to applicable laws and regulations related to the processing of personal information. When determining the adjustment in the PIMS, the top management shall take the following into account and make adjustments accordingly:

		(1) The review report. (2) Changes in social situation, public awareness, and technological development. (3) Changes in the scope of business. (4) Internal and external recommendations for improvements. (5) Changes that may affect the PIMS.
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	**NDCR r 6.3 Risk and Planning** When planning to establish a PIMS, the organization should: (11) consider external and internal issues. (12) consider needs and expectations of stakeholders. (13) consider relevant laws and regulations. (14) plan risk management principles and procedures. (15) identify risks and measures. The organization may adopt principles of privacy by design and default.

		NDCR r 6.3.1 Risk Analysis The organisation should establish risk analysis procedures which should include: (13) establish principles related to risk, including risk analysis and management principles. (14) ensure that each risk analysis conducted produces consistent, effective and comparative results. (15) identify risks and who is subjected to the risk. (16) analyse risks, including identifying the consequences, the likelihood of occurrence and the degree of the risk. (17) evaluate risks, including comparing the outcome of the analysis and determine the priority in which each risk is to be dealt with. (18) identify the impact the risk has on the organisation and data subjects. **NDCR r 6.3.2 Risk Management**

		The organization shall utilize the outcome of its risk analysis to determine appropriate measures to manage its risks, and shall comply with Annexure A. **NDCR r 9.2 Internal Evaluation** An organization shall carry out the annual internal evaluation in order to understand whether the PIMS complies with the following requirements: (1) Applicable laws and the NDCR. (2) Personal information protection and administration policy, manual, and related specific rules. An organization shall plan the way and procedures of internal evaluation in order to determine the principle, scope, frequency and method of internal evaluation. An organization shall compile the written report on the planning, implementation, reports, improvements, and follow-up of internal evaluation. An internal evaluation plan shall be planned by an internal auditor or verifier of the domestic certification system, who is responsible to ensure the effectiveness of internal evaluation and compile the internal evaluation report.

		NDCR r 4.1 External and Internal Issues The organisation shall determine external and internal issues that relate to the implementation of its PIMS and that could affect the effective operation of its PIMS. **NDCR r 4.2 Needs and expectations of Stakeholders** The organisation shall identify stakeholders to the PIMS and their needs and expectations. **NDCR r 9.3 Regular Review** To implement the personal information protection and management, the personal information management representative shall convene the review meeting every year on a regular basis to review the PIMS, compile the written report, and report the related resolutions to the top management. The regularly held review meeting shall review the following and compile a review report:

		(1) Implementation and analysis of PIMS. (2) Effect of corrective and preventive actions. (3) Result of effectiveness measurement. (4) Amendments to applicable laws and regulations related to the processing of personal information. When determining the adjustment in the PIMS, the top management shall take the following into account and make adjustments accordingly: (1) The review report. (2) Changes in social situation, public awareness, and technological development. (3) Changes in the scope of business. (4) Internal and external recommendations for improvements. (5) Changes that may affect the PIMS. **NDCR r 10.1 General Principle**

		According to the result of internal evaluation, an organization shall plan and implement corrective and preventive actions. **NDCR r 10.2 Corrective actions** To direct against potential risk of incompliance, an organization shall plan and complete the corrective actions and the following: (1) Confirming the content of incompliance and determining the cause (2) Evaluating demands and proposing the corrective actions to ensure the absence of occurrence of incompliance. (3) Setting up a proper period for execution. (4) Recording the result of corrective actions. (5) Reviewing the result of corrective actions. **NDCR r 10.3 Preventive actions**

		An organisation shall determine the risk potential incompliances occurring, and shall develop a plan and take action to prevent its occurrence. The organization shall: (1) identify potential incompliances that may arise due to identified risks; (2) develop a plan to prevent incompliances from occurring; (3) determine an implementation time; (4) keep records; (5) review the outcome; (6) continuously improve its PIMS.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access,	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information.	**NDCR r 8.10 Emergency response** To avoid potential disadvantages and impacts arising from accidents, an organization shall formulate the emergency response measures, which shall at least include: (1) Proper notification upon investigation and provision of channels for subsequent queries and processing. (2) Measures that prevent the damage from expanding.

destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of	The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	(3) Measures that prevent the occurrence of similar accidents. (4) Submission of the report on the accident to the grant authority. **NDCR r 8.7 Security Measures** An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures. (2) technical measures. **NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization** When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should:

the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		(1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information. (7) maintain a right to give directions to other organizations regarding how to manage personal information.

		(8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* ('PDPA')
36. Upon request, do you provide confirmation of whether or not you hold	Where the Applicant answers **YES**, the Accountability Agent must verify that the	**NDCR r 8.5.1 Related rights of personal information**

personal information about the requesting individual? Describe below.	Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted.	An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r. 8.5.2 Procedures to exercise data subject rights** An organization shall have relevant procedures to ensure that data subject rights are exercised, and should at least include the following: (1) establish procedures which allow data subjects to exercise their rights; (2) establish mechanisms to affirm the identity of data subjects; (3) determine whether an request to exercise data subject rights may be refused according to law; (4) provide contact information, enabling data subjects to make a complaint in regards to disputes arising from the exercise of their rights; (5) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights within the statutory period;

	Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(6) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights. Upon refusal, provide reasons and give notice; (7) provide reasons and notice, if the organization decides to extend time to make a decision as to whether to grant or refuse to grant the data subject to exercise its rights; (8) retain records.
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the	**NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.2 Procedures to exercise data subject rights**

access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable	appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	An organization shall have relevant procedures to ensure that data subject rights are exercised, and should at least include the following: (1) establish procedures which allow data subjects to exercise their rights. (2) establish mechanisms to affirm the identity of data subjects. (3) determine whether an request to exercise data subject rights may be refused according to law. (4) provide contact information, enabling data subjects to make a complaint in regards to disputes arising from the exercise of their rights. (5) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights within the statutory period. (6) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights. Upon refusal, provide reasons and give notice. (7) provide reasons and notice, if the organization decides to extend time to make a decision as to whether to grant or refuse to grant the data subject to exercise its rights. (8) retain records.

(in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed,	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy.	**NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination

amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or	If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of	of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.2 Procedures to exercise data subject rights** An organization shall have relevant procedures to ensure that data subject rights are exercised, and should at least include the following: (1) establish procedures which allow data subjects to exercise their rights. (2) establish mechanisms to affirm the identity of data subjects. (3) determine whether an request to exercise data subject rights may be refused according to law. (4) provide contact information, enabling data subjects to make a complaint in regards to disputes arising from the exercise of their rights. (5) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights within the statutory period. (6) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights. Upon refusal, provide reasons and give notice.

where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction	written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(7) provide reasons and notice, if the organization decides to extend time to make a decision as to whether to grant or refuse to grant the data subject to exercise its rights. (8) retain records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.

will not be provided, together with contact information for further inquiries about the denial of access or correction?		

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** NDCR and *the Personal Data Protection Act* ('PDPA')
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. ● Internal guidelines or policies (if	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	**NDCR r 5.2 Personal Information Protection and Administration policies** Top management shall establish a personal information management policy that: (1) addresses relevant laws and regulations. (2) includes the purpose and objective of establishing a PIMS.

applicable, describe how implemented) _____ ● Contracts _____ ● Compliance with applicable industry or sector laws and regulations ____ ● Compliance with self-regulatory applicant code and/or rules ____ ● Other (describe) ____		(3) includes a commitment to continue to improve the PIMS. The PIMS policy shall: (1) be in writing (2) be communicated within the organization. **NDCR r 6.2 Personal information protection and administration manual** To establish a PIMS, an organization shall compile a personal information protection and administration manual specifying the rules and effective measures for the operations of the system. Specific rules shall at least include: (1) Applicable acts and related regulations. (2) Identification of all personal information kept by the enterprise. (3) Matters of collection, processing and use of personal information by the enterprise.

		(4) Risk analysis and control measures related to personal information. (5) Emergency responses to accidents. (6) Authorization and responsibility of personal information management possessed by each department and level in an organization. (7) Exercise of rights of party. (8) Maintenance of correct personal information. (9) Safety management measures. (10) Supervision and rewards and punishments of personnel. (11) Supervision of commissioned collection, processing or use of personal information. (12) Training. (13) Management of documents and records related to PIMS. (14) Complaints and consultation. (15) Internal evaluation. (16) Corrective and preventive actions.

		(17) Regular review of the top management. (18) A personal information or information security system protection plan. **NDCR r 8.1 Applicable acts and related regulations** An organization shall identify the applicable acts and explicitly reveal the consistency between the internal PIMS and related domestic personal information protection laws in terms of content and implementation. An organization shall also adjust the internal PIMS according to changes in applicable laws and regulations. **NDCR r 9.3 Regular Review** To implement the personal information protection and management, the personal information management representative shall convene the review meeting every year on a regular basis to review the PIMS, compile the written report, and report the related resolutions to the top management. The regularly held review meeting shall review the following and compile a review report:

		(1) Implementation and analysis of PIMS. (2) Effect of corrective and preventive actions. (3) Result of effectiveness measurement. (4) Amendments to applicable laws and regulations related to the processing of personal information. When determining the adjustment in the PIMS, the top management shall take the following into account and make adjustments accordingly: (1) The review report. (2) Changes in social situation, public awareness, and technological development. (3) Changes in the scope of business. (4) Internal and external recommendations for improvements. (5) Changes that may affect the PIMS.
40. Have you appointed an individual(s) to be responsible for your	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is	**NDCR r 5.1 Top Management** Top management shall have the following responsibilities:

overall compliance with the Privacy Principles?	responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	(1) Determine the objective of the PIMS, ensuring that the objective aligns with the mission and goals of the organization. (2) Determine personal information protection and policies. (3) Determine resources. (4) Determine the structure and responsibilities of the personal information protection team. (5) Regularly review the effectiveness of the PIMS. (6) Establish an effective communications mechanism, ensuring education and support is provided in a timely manner. (7) Communicate the importance of implementing a PIMS. **NDCR r 7.4 Communication** An organization shall establish mechanisms to effectively communicate information to its personnel. **NDCR r 5.4 Representative of top management**

		The top management shall assign one member to serve as the representative of personal information protection and management system, who shall have the following duties and responsibilities: (1) Maintain the effective operation of PIMS and establish a necessary personnel structure. (2) Ensure the impartiality and objectiveness of performance of duties. (3) Ensure the establishment, implementation, and maintenance of procedures required in the PIMS. (4) Report the implementation of and improvement mechanism for the PIMS to the top management. **NDCR r 5.5 Personal information administrator** An organization shall assign the personal information administrator that is equipped with one of the following qualifications to promote and ensure the effective operation of PIMS: (1) administrator of the domestic certification system. (2) internal auditor of the domestic certification system.

		(3) verifier of the domestic certification system.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 5） A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 6） A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 7） A formal complaint-resolution process; AND/OR	**NDCR r 8.5.1 Related rights of personal information** An organization shall formulate the rules and procedures of inquiry, read, supplement, correction, reproduction, termination of collection, termination of processing, termination of use, deletion of personal information, and complaints and consultation and keep related records. **NDCR r 8.5.2 Procedures to exercise data subject rights** An organization shall have relevant procedures to ensure that data subject rights are exercised, and should at least include the following: (1) establish procedures which allow data subjects to exercise their rights. (2) establish mechanisms to affirm the identity of data subjects. (3) determine whether an request to exercise data subject rights may be refused according to law. (4) provide contact information, enabling data subjects to make a complaint in regards to disputes arising from the exercise of their rights.

	8） Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	(5) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights within the statutory period. (6) make a decision as to whether the organization grants or refuses to grant the data subject to exercise its rights. Upon refusal, provide reasons and give notice. (7) provide reasons and notice, if the organization decides to extend time to make a decision as to whether to grant or refuse to grant the data subject to exercise its rights. (8) retain records. **NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal

		information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	**NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly. (2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	**NDCR r 8.5.3 Complaints and consultation** An organization shall meet the following requirements for disposal of complaints and consultation: (1) Rely to the party properly and swiftly.

		(2) Report the case to the personal information management representative depending on the content of complaints and consultation; the personal information management representative is responsible to determine the content and way of reply. (3) Keep records of matters specified in the preceding two paragraphs.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	**NDCR r 7.2.1 General Principle** An organization shall ensure that its personnel has adequate skills and knowledge in regards to its PIMS and reward system. **NDCR r 7.2.2 Basic training** An organization shall provide necessary training programs regarding the personal information management for the personnel. **NDCR r 7.2.3 Training for authorized personnel** An organization shall determine the necessary capabilities of the authorized personnel related to the PIMS and plan the implement the training programs subject to demands.

		NDCR r 7.2.4 Record and improvement An organization shall keep records and set up improvement mechanisms for training programs provided for the personnel.
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers **YES, the** Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	**NDCR r 6.2 Personal information protection and administration manual** To establish a PIMS, an organization shall compile a personal information protection and administration manual specifying the rules and effective measures for the operations of the system. Specific rules shall at least include: (1) Applicable acts and related regulations. (2) Identification of all personal information kept by the enterprise. (3) Matters of collection, processing and use of personal information by the enterprise. (4) Risk analysis and control measures related to personal information. (5) Emergency responses to accidents.

		(6) Authorization and responsibility of personal information management possessed by each department and level in an organization. (7) Exercise of rights of party. (8) Maintenance of correct personal information. (9) Safety management measures. (10) Supervision and rewards and punishments of personnel. (11) Supervision of commissioned collection, processing or use of personal information. (12) Training. (13) Management of documents and records related to PIMS. (14) Complaints and consultation. (15) Internal evaluation. (16) Corrective and preventive actions. (17) Regular review of the top management. (18) A personal information or information security system protection plan.

		NDCR r 8.1 Applicable acts and related regulations An organization shall identify the applicable acts and explicitly reveal the consistency between the internal PIMS and related domestic personal information protection laws in terms of content and implementation. An organization shall also adjust the internal PIMS according to changes in applicable laws and regulations. **NDCR r 8.4.4 Use** An organization shall meet the following requirements for use of personal information: (1) Use personal information within the necessary scope of specific purpose of collection. (2) Use personal information outside the purpose in accordance with the applicable laws. (3) Keep records of matters specified in the preceding two paragraphs.

		Article 16 of PDPA Except for the personal data specified under Paragraph 1, Article 6, a government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on certain bases. Please see the following link for the full list of bases: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 **Article 20, Paragraph 1 of PDPA** Except for the personal data specified in Paragraph 1, Article 6, a non-government agency shall use personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: 1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject;

		4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests.
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	**NDCR r 8.8 Supervision of personnel** An organization shall take necessary and proper monitoring measures for collection, processing, and use of personal information. **NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization** When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties.

● Internal guidelines or policies _____ ● Contracts _____ ● Compliance with applicable industry or sector laws and regulations _____ ● Compliance with self-regulatory applicant code and/or rules _____ ● Other (describe) _____		(2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information. (7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs.

		(9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: ● Abide by your APEC-compliant privacy policies and	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	**NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization** When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification.

practices as stated in your Privacy Statement? _____ ● Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____ ● Follow instructions provided by you relating to the manner in which your personal information must be handled? _____ ● Impose restrictions on subcontracting		(3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information. (7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends.

unless with your consent? _____ ● Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ ● Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? ● Other (describe) _____		(10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.
48. Do you require your personal information processors, agents,	The Accountability Agent must verify the existence of such self-assessments.	**NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization**

contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.		When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information.

		(7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.
49. Do you carry out regular spot checking or monitoring of your personal information	Where the Applicant answers **YES**, the Accountability Agent must verify the existence	**NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization**

processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures. (5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information.

		(7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations, other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.
50. Do you disclose personal information to other recipient **persons or organizations** in	If **YES**, the Accountability Agent must ask the Applicant to explain:	**NDCR r 8.7 Security Measures** An organization shall adopt appropriate and necessary security measures according to the risks that it may face when it collects, processes, and uses

situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	(1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	personal data, in order to prevent data breaches. According to Annexure A, appropriate and necessary security measures include but are not limited to: (1) organisational measures. (2) technical measures. **NDCR r 8.9 Supervision of other organizations that collect, process, or use personal information on behalf of the organization** When other organizations carry out all or part of the processing on behalf of the organization, the organization shall establish selection and supervision standards. The organization should: (1) identify the rights and obligations of both parties. (2) select an organization that adopts safety measures or has obtained third party certification. (3) identify the scope, the category, the purpose of the personal information that is to be collected, processed and used, and how long the personal information is to be retained. (4) ensure that other organizations adopt security measures.

		(5) ensure that if other organizations select further organizations to process personal information, the scope of processing is identified. The organization must give consent, and further organizations should adopt safety measures. (6) ensure that other organizations regularly report to the organization of how it manages personal information. (7) maintain a right to give directions to other organizations regarding how to manage personal information. (8) ensure that other organizations should immediately report to the organization, and put in place adequate remedies when a data breach occurs. (9) require other organizations to return all relevant documents and media to the organization and delete all relevant personal information, when their relationship ends. (10) ensure that other organizations shall only collect, use, process personal information under the direction of the organization. If other organizations are of the view that the direction contradicts any laws or regulations,

		other organizations should communicate this to the organization immediately. The organization shall conduct regular review on other organisations and keep records.

Annexure A: Security Measures

Annexure A is a set of security measures supplementary to the requirements of the domestic certification system. Organizations must satisfy all security measures listed under Annexure A in order to pass APEC CBPRs certification. This is to ensure that organizations comply with domestic laws and regulations, and have implemented appropriate security measures to prevent data breaches.

A8.7 Information Security	
A8.7.1 Access control	Objective: To ensure that access of personal information is internally regulated and protected, preventing unauthorized access or destruction of personal information. Measures: 1. Implementing access control The organization shall establish access control policies and mechanisms (e.g. an access control list) to control the access of personal information. 2. Account management The organization shall establish account management mechanisms, including procedural rules on applying, creating, suspending, and terminating accounts. The organization shall terminate or cease to use accounts that have lapsed, are temporary or are unused. When the organization has set an expiry date of an account, upon expiry, its system should automatically sign out the user. 3. Roles and Responsibilities The organization shall define and allocate roles and responsibilities in regards to access control. 4. Access Minimization User access shall follow the principle of access minimization, where all access should be restricted and controlled, providing users enough access that enables then to complete allocated tasks. 5. Remote Access

	The organization shall establish policies prohibiting or restricting remote access of personal information. If remote access is permitted, the organization shall adopt encryption methods and implement automatic monitoring mechanisms to ensure policies are complied with. 6. Mobile Access The organization shall establish policies prohibiting or restricting using mobile devices to access personal information. If mobile access is permitted, the organization shall ensure that mechanisms are in place to protect the mobile device. The security of the mobile device shall be assessed regularly. 7. Information Sharing The organization shall establish information sharing mechanisms, ensuring that delegated access complies with access control policies.
A8.7.2 Technical Compliance	Objective: To determine what should be audited and what records should be kept, according to risk analysis conducted on the information system and business needs of the organization. To establish supervision mechanisms accordingly. Measures: 1. Auditing Incidents The organization shall monitor incidents that are likely to create a risk to the confidentiality of personal information, for example, when the access of personal information is not authorized.

	2. Auditing Reports The organization shall regularly review and evaluate auditing reports of information systems, in order to identify inappropriate or abnormal activities, and to inspect on activities that are likely to be breaches. The organization shall provide its auditing report to responsible officers and implement appropriate measures.
A8.7.3 Identification and Authentication	Objective: To establish methods to affirm the accounts and access rights of internal users in order to ensure accountability. Measures: 1. Identification and authentication of users Every user shall have only one account. The information system shall have mechanisms to identify and authenticate a user's identity, preventing the sharing of accounts. 2. Management of user identity When a user logs into the information system with a default password, a password change shall be required. Any information relating to the user's identity (e.g. passwords) shall not be transferred without encryption.
A8.7.4 Media Safety	Objective: To ensure the safe access, preservation, transfer and elimination of media on which personal information is stored. Measures:

	Media Access The organization shall implement measures to restrict the access of digital and non digital media and shall restrict media access to specific persons. Media Labelling The organization shall develop labelling methods and label its media. Media Storage The organization shall establish and implement procedures to ensure media is safety stored. Media Transfer and Delivery Appropriate security measures shall be implemented in regards to media that stores personal information when such media is delivered or transferred to areas outside the control of the organization. Media Disposal The organization shall establish procedures to ensure that media is disposed of safely and cannot be restored.
A8.7.5 Physical and Environmental Security	Objective: To prevent unauthorized physical access into spaces where personal information is stored, which could cause data breach. Measures: 1. Control The organization shall identify security perimeters, implement appropriate security measures to protect the

	physical space and environment where personal information is stored, and adopt entry controls. 2. Review The organization shall regularly review the effectiveness of its security measures and establish security mechanisms to control the physical spaces and environment in which personal information is stored.
A8.7.6 Information transfer	Objective: To prevent unauthorized disclosure of personal information when transferred. Measures: 1. Boundary Protection The organization shall determine the external and internal boundaries of the information system and establish appropriate supervision and controlling measures to protect boundaries. 2. Confidentiality of transfers The organization shall implement appropriate measures to ensure that the transfer of personal information is confidential.
A8.7.7 Integrity of Systems and Information	Objective: To ensure the effectiveness of security measures implemented in information systems. Measure: 1. Security Review The organization shall identify technical vulnerabilities of its information system and report and rectify. The organization shall test the information system before it

	is updated, in order to understand the likely consequences. 2. Auditing The organization shall ensure that its information system is developed in a way that enables it to be audited – alterations in the information system can be identified, logging records can be extracted. The information system should have separate interfaces that manage information, allowing the organization to extract relevant information when investigating an incident. Access rights should also be restricted to certain users. 3. Malware Protection The organization shall put in place malware protection mechanisms on possible endpoints, workstations, servers or portable media related to its information system. 4. Supervision The organization shall monitor internal and external transfers via its information system. When the organization is aware of a cyberattack, it shall follow procedures and report to responsible persons.
A8.7.8 Software Development Life Cycle	Objective: To ensure that the development of the information system is secure, preserving the confidentiality, integrity and availability of information. Measures: The organization shall adopt the Secure Software Development Life Cycle (SSDLC) principle when

	identifying needs, designing, developing, testing, and operating the information system.
A8.7.9 Secure Software Development Life Cycle – Other Organizations	Objective: To ensure that the development of the information system is safely managed when other organizations are engaged to develop the information system. Measures: If other organizations are engaged to develop the information system, the organization shall ensure that concepts of confidentiality, integrity and availability are reflected in the Secure Software Development Life Cycle, and should be incorporated into a contract.
A8.7.10 Establish Developing, Testing and Operating Mechanisms	Objective: To ensure that information flow mechanisms and information management mechanisms are established. Measures: The organization shall separate the developing, testing and operating phases of the information system. The organization shall refrain from using real personal information for testing. If real personal information must be used for testing, permission must be obtained, where procedures must be developed and records kept.

A8.7.11 Business Continuity Plan	Objective: To ensure that the organization continues to operate properly when information system incidents occur, a Maximum Tolerable Period of Disruption (MTPD) and Minimum Acceptable Service Level shall be determined. Measures: 1. Information Backup The organization shall determine the period of time which information losses can be tolerated, and accordingly, back up information and source codes. The organization shall regularly review backup information to ensure that the media used is reliable and the backup information is accurate. 2. System Backup The organization shall determine a Maximum Tolerable Period of Disruption in the event of an information system disruption. Before the disruption has been resolved and within the MTPD, the information system should be backed up by other systems ensuring that a Minimum Acceptable Service Level is maintained.
A8.8 Management and Supervision of Personnel	
A8.8.1 Employment	Objective: To ensure that employees and contractors are suited for their roles. Measures: The organization shall carefully select employees or contractors according to the roles and responsibilities required.

A8.8.2 Confidentiality Agreement	Objective: To ensure that responsibilities are understood. Measures: The contract of employment shall include a confidentiality agreement which relates to personal information protection. The confidentiality agreement should require a duty of confidentiality to extend for a period of time after the termination of employment.
A8.8.3 Education	Objective: To ensure that information security education is provided, to continuously operate and improve the information system. Measures: The organization shall develop plans for educational training and assessment mechanisms to assess its effectiveness.

ANNEX 4: GUIDELINE FOR THE OPERATION OF DISPUTE RESOLUTION MECHANISM OF THE DOMESTIC CERTIFICATION SYSTEM

0. Regulatory Basis

These Guidelines are instituted according to the "Operational Regulations of the Domestic Certification System" (hereinafter referred to as the "Operational Regulations")

1. Purpose

These Guidelines are instituted as the rules to be followed to ensure the effective implementation and the accuracy of the introduction of the Domestic Certification System in enterprises.

2. Definition

Unless otherwise provided, all the terms used in these Guidelines shall follow the terms defined in the Operational Regulations and the Domestic Certification System requirements.

3. Dispute Resolution Procedure

3.1 Dispute Acceptance and Notification

3.1.1 Any person noticing that the labeling organization breaches the regulations of the Domestic Certification System may file a complaint with the Domestic Certification System Operation Agency by phone or e-mail, or by filling the counseling service form on the official website of the Domestic Certification System.

3.1.2 The Domestic Certification System Operation Agency shall investigate generally if the complaint is governed by the regulations of the Domestic Certification System within seven working days after the receipt of the complaint. If the dispute of the complaint is governed by the regulations of the Domestic Certification System, the Domestic Certification System

Operation Agency shall promptly notify the complainant and the accused labeling organization in writing.

3.2 Dispute Investigation

3.2.1 The Domestic Certification System Operation Agency shall complete the dispute investigation within one month after notifying the complainant and the labeling organization; provided, however, that if the dispute is complicated, the aforementioned period may be extended once, if necessary, and the Domestic Certification System Operation Agency shall notify the complainant and the labeling organization of the reason for extension in writing.

3.2.2 For the purpose of investigation, the Domestic Certification System Operation Agency may carry out the investigation by using the following methods:

(1) Asking the labeling organization or the complainant to specify the details of the dispute.

(2) Inquiring the opinions of the competent authority and the authority responsible for the legal interpretation of the Personal Data Protection Act for the labeling organization.

(3) Asking for the assistance of other Accountability Agents of the APEC CBPR system.

(4) Other useful activities for the fulfillment of the purpose of investigation.

3.3 Dispute Resolution

3.3.1 The complainant and the labeling organization shall be informed of the result of the dispute investigation in writing.

3.3.2 If the labeling organization is found in breach of the regulations of the Domestic Certification System according to the result of dispute investigation, the following procedures shall be applied:

(1) Asking the labeling organization to rectify the breach within a certain period. The right of the organization to use the label of data privacy protection shall be suspended during the rectification period. The aforementioned period shall not exceed three months or the term of the label.

(2) After the labeling organization completes the rectification, the Domestic Certification System Operation Agency shall review and confirm, by itself or by an entrusted certification body, if the regulations of the Domestic Certification System are met after the rectification.

(3) The Domestic Certification System Operation Agency shall notify the person involved and the labeling organization of the result of rectification in writing.

(4) If the labeling organization fails to complete the rectification within the period, the right of the labeling organization to use the label of data privacy protection shall be terminated.

4. Records, Compilation and Publication

4.1 The Domestic Certification System Operation Agency shall preserve the information with respect to dispute resolution, and the contents thereof shall include at least the complainant, the time the complainant files the complaint, dispute investigation and the dispute resolution.

4.2 The Domestic Certification System Operation Agency shall compile the amount of disputes, types of disputes, the involved provisions of the regulations of the Domestic Certification System and the handling of disputes, publicize them on the official website of the Domestic Certification System, and notify the legal interpretation authority of the *Personal Data Protection Act* and the Joint Oversight Panel of the APEC CBPR System.

4.3 The Domestic Certification System Operation Agency shall publicize the handling of remarkable complaints, including the interpretation to the regulations of the Domestic Certification System and the suggestion to practical operation, on the official website of the Domestic Certification System in an anonymous way.

5. Protection of the Right of Complainant

5.1 The complainant shall not be prejudiced for the filing of the complaint.

5.2 For the purpose of dispute investigation, the Domestic Certification System Operation Agency may, by acquiring the prior consent of the complainant, provide the information of the complainant to the labeling organization within a necessary scope.

6. Supplemental Provision

6.1 These Guidelines shall be submitted to the Ministry of Economic Affairs for reference and for promulgation and enforcement; the same shall apply to any amendment hereof.