Annex B

*KISA has developed our CBPRs assessment criteria making use of assessment checklist of our domestic Privacy Certification System, 'Personal Information & Information Security Management System(ISMS-P)', for demonstrating that it meets the baseline of APEC CBPRs Program Requirements.*

**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.*

※ The number(*) came from the numbers on the ISMS-P and PIMS checklist

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | Program Requirement of KISA |
|---|---|---|
| 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 statements and/or hyperlinks to the same. | If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics:<br>• 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).<br>• Is in accordance with the principles of the APEC Privacy Framework;<br>• Is easy to find and accessible. | 3.5.1.1* Do you continuously update and disclose the personal information processing policy in such a way that the information subject (user) can check it easily? |

| **Question** (*to be answered by the Applicant Organization*) | **Assessment Criteria** (*to be verified by the Accountability Agent*) | Program Requirement of KISA |
|---|---|---|
| | • Applies to all personal information; whether collected online or offline.<br>States an effective date of Privacy Statement publication.<br>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.a) Does this privacy statement describe how personal information is collected? | If **YES**, the Accountability Agent must verify that:<br>• The statement describes the collection practices and policies applied to all | 3.5.1.2 Does the personal information processing policy include all matters required by the law? |

| **Question** (*to be answered by the Applicant Organization*) | **Assessment Criteria** (*to be verified by the Accountability Agent*) | Program Requirement of KISA |
|---|---|---|
| | covered personal information collected by the Applicant.<br>• the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and<br>• The Privacy Statement reports the categories or specific sources of all categories of personal information collected.<br>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. | |

| **Question** (*to be answered by the Applicant Organization*) | **Assessment Criteria** (*to be verified by the Accountability Agent*) | Program Requirement of KISA |
|---|---|---|
| | 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 purpose for which the personal information will or may be made available.<br>Where the Applicant answers **NO** and does not identify an applicable qualification, the | |

| **Question** (*to be answered by the Applicant Organization*) | **Assessment Criteria** (*to be verified by the Accountability Agent*) | Program Requirement of KISA |
|---|---|---|
| | 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 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.<br>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 | |

| **Question** (*to be answered by the Applicant Organization*) | **Assessment Criteria** (*to be verified by the Accountability Agent*) | Program Requirement of KISA |
|---|---|---|
| | 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. | |
| 1.f) Does this privacy statement provide information | Where the Applicant answers **YES**, the Accountability Agent must verify that the | |

| **Question** (***to be answered by the Applicant Organization***) | **Assessment Criteria** (***to be verified by the Accountability Agent***) | Program Requirement of KISA |
|---|---|---|
| regarding whether and how an individual can access and correct their personal information? | Privacy Statement includes:<br>• The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means).<br>• The process that an individual must follow in order to correct his or her personal information<br>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, | |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | Program Requirement of KISA |
|---|---|---|
| | the 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.<br>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. | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases where there are special provisions in the law? |
| | | 3.1.2.2 Is the method and time of obtaining the consent of the information subject (user) appropriately established? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | Program Requirement of KISA |
|---|---|---|
| 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 indicate the purpose(s) for which personal information is being collected? | 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 link from URL, attached documents, pop-up window, or other.<br><br>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. | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases where there are special provisions in the law? |
| | | 3.3.1.1 If personal information is provided to a third party, unless prescribed in laws, do you clearly the details to the information subject (user) and obtain his/her consent? |

| **Question** (***to be answered by the Applicant Organization***) | **Assessment Criteria** (***to be verified by the Accountability Agent***) | Program Requirement of KISA |
|---|---|---|
| 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.<br><br>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. | 3.3.1.1 If personal information is provided to a third party, unless prescribed in laws, do you clearly the details to the information subject (user) and obtain his/her consent? |

**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*)** | **Program Requirement of KISA** |
|---|---|---|
| 5. How do you obtain personal information:<br>5.a) Directly from the individual?<br>5.b) From third parties collecting on your behalf?<br>5.c) Other. If YES, describe. | The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information.<br>Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard.<br>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. | 1.2.2.2 Do you identify the current status of personal information processing within the scope of the management system, identify the flow of personal information and document, e.g. the personal information flow chart? |
| 6. Do you limit your personal | Where the Applicant answers **YES** and | 3.1.1.1 If personal information is collected, do you |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| 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? | 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:<br>• Each type of data collected<br>• The corresponding stated purpose of collection for each; and<br>• All uses that apply to each type of data<br>• An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection.<br>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 | collect only minimum information necessary for service provision or information processing according to laws?<br>3.1.5.3 If it is necessary for implementation of the service contract, do you apply the minimum collection principle even if the personal information (details of use, etc.) is collected and generated by an automatic collection system when the business operator is providing service? |

| **Question** (***to be answered by the Applicant Organization***) | **Assessment Criteria** (***to be verified by the Accountability Agent***) | **Program Requirement of KISA** |
|---|---|---|
| | 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. | |
| 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.<br>Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle. | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases where there are special provisions in the law? |
| | | (Addition) Does the law allow collection of personal information without consent? |

**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 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*)** | **Program Requirement of KISA** |
|---|---|---|
| 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 provided at the time of collection, to those purposes for which the information | 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 effect at the time of collection or for other compatible or related purposes. | 3.2.5.1 When personal information is collected for the first time, do you use and provide it only for the purposes to which the information subject (user) consented or to the extent based on laws? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| was collected or for other compatible or related purposes? If necessary, provide a description in the space below. | Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below. | |
| 9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.<br>9.a) Based on express consent of the individual? | 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:<br>• Online at point of collection<br>• Via e-mail | 3.2.5.2 If you use or provide personal information in excess of the collection purpose or scope, do you obtain additional consent from the information subject (user) or limit it to cases where there are legal grounds? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| 9.b) Compelled by applicable laws? | • Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify).<br><br>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.<br><br>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.<br><br>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 | |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle. | |
| 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 requested by the individual, or compelled by law.<br>Also, the Accountability Agent must require the Applicant to identify:<br>1) each type of data disclosed or transferred; | 3.3.1.1 If personal information is provided to a third party, unless prescribed in laws, do you clearly the details to the information subject (user) and obtain his/her consent? |
| 11. Do you transfer personal information to personal information processors? If YES, describe. | | 3.3.2.1 If personal information processing is outsourced to a third party, do you disclose up-to-date information on the details of the outsourced jobs and the outsourcee, on the Internet homepage, etc.? |
| | | 3.3.2.2 If it is necessary to obtain consent to the outsourcing of personal information processing, do you notify information on the outsourcee and the details of |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 2) the corresponding stated purpose of collection for each type of disclosed data; and<br>3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.).<br>Usingtheabove,theAccountabilityAgentmustverifythattheApplicant'sdisclosuresortransfersofallpersonalinformationislimitedtothepurpose(s)ofcollection,orcompatibleorrelatedpurposes. | outsourced jobs and obtain consent? |
| 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. | | 3.3.1.3 If personal information is provided to a third party, do you provide only minimum personal information items fit for the purpose of provision? |
| | | (Additional) If personal information processing is outsourced, do you obtain consent from the information subject (user), or use the personal information for the notified purposes only, and collect only the minimum personal information items? |
| 13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?<br>13.a) Based on express consent of the individual? | 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.<br>Where the Applicant answers YES to 13.a, the Accountability Agent must require the Applicant to provide a description of how | 3.2.5.2 If you use or provide personal information in excess of the collection purpose or scope, do you obtain additional consent from the information subject (user) or limit it to cases where there are legal grounds? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| 13.b) Necessary to provide a service or product requested by the individual?<br><br>13.c) Compelled by applicable laws? | individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify)<br><br>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. | |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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.<br><br>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. | |

**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*)** | **Program Requirement of KISA** |
|---|---|---|
| 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:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases where there are special provisions in the law? |
| | | 3.1.1.2 If you collect personal information other than the minimum information necessary for the purposes of collection, do you allow the information subject (user) to choose whether to provide such personal information? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | • Other (in case, specify)<br>The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated<br>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. | |
| 15. Subject to the qualifications described below, do you provide a mechanism | Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below. | mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify)<br>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 | where there are special provisions in the law?<br>3.1.1.2 If you collect personal information other than the minimum information necessary for the purposes of collection, do you allow the information subject (user) to choose whether to provide such personal information? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:<br>• 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<br>• Personal information may be disclosed or distributed to third parties, other than Service Providers.<br>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.<br>Where the Applicant answers NO and does not identify an acceptable qualification, the | |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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. | |
| 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:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify) | 3.3.1.1 If personal information is provided to a third party, unless prescribed in laws, do you clearly the details to the information subject (user) and obtain his/her consent? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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:<br>• 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.] | |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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.<br>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. | |
| 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 | Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner .<br>Where the Applicant answers NO, or when | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases where there are special provisions in the law? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| their personal information, are they displayed or provided in a clear and conspicuous manner? | 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. | |
| 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.<br><br>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 | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases where there are special provisions in the law?<br><br>3.1.2.3 When receiving written consent (including electronic documents) from the information subject (user), do you clearly mark the important information prescribed by laws and make it easy to see? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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. | |
| 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.<br>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 | 3.1.2.1 When collecting personal information, do you clearly notify relevant information to the information subject (user) and obtain his/her consent except for cases where there are special provisions in the law? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | be easily accessible and affordable in order to comply with this principle. | |
| 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.<br>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.<br>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. | (Addition) If the information subject (user) exercises his/her option with regard to the collection, use and provision of personal information, do you have and implement the procedure for immediately handling it? |

**INTEGRITY OF PERSONAL INFORMATION**

**Assessment Purpose -** *The questions in this 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*)** | **Program Requirement of KISA** |
|---|---|---|
| 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.<br>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.<br>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to verify and ensure | 3.2.2.1 Do you manage collected personal information safety according to the internal procedure, and keep it up-to-date? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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.<br>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures/steps to verify and | 3.2.2.2 Do you provide a method of enabling the information subject (user) to maintain the accuracy, completeness and up-to-dateness of personal information? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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. | |
| 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 transferred? 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 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.<br>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 | (Addition) If personal information is outsourced or provided to a third party, do you take measures with regard to correction and withdrawal of deletion and check the results? (PIMS 6.1.2.4) |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | or other service providers acting on the Applicant's behalf.<br>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 personal information was disclosed? | 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.<br>The Accountability Agent must verify that these procedures are in place and operational.<br>Where the Applicant answers NO, the Accountability Agent must inform the | (Addition) If personal information is outsourced or provided to a third party, do you take measures with regard to correction and withdrawal of deletion and check the results? (PIMS 6.1.2.4) |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| 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. | |
| 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.<br>The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being | (Addition) Is there a procedure for receiving notification that the personal information outsourced or provided to a third party is incorrect, incomplete or not updated? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | made by the Applicant and by the processors, agents or other service providers.<br><br>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. | |

**SECURITY SAFEGUARDS**

**Assessment Purpose -** *The questions in this 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*)** | **Program Requirement of KISA** |
|---|---|---|
| 26. Have you implemented an information security policy? | Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy.<br>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. | 1.1.5.1 Do you establish the highest-level information protection and personal information protection policies, including the grounds of all information protection and personal information protection activities conducted by the organization? |
| | | 1.1.5.2 Do you establish the guideline, procedure and manual that prescribe the detailed method, procedure and cycle necessary for implementing information protection and personal information protection policies? |
| 27. Describe the physical, technical and administrative safeguards you have implemented to protect personal | Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must | (Addition) Do you have and carry out the internal control plan which includes the details of technical, administrative and physical measures to protect personal information? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses? | verify the existence of such safeguards, which may include:<br>• Authentication and access control (eg password protections)<br>• Encryption<br>• Boundary protection (eg firewalls, intrusion detection)<br>• Audit logging<br>• Monitoring (eg external and internal audits, vulnerability scans)<br>• Other (specify)<br>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 | - providing education<br>- access control<br>- preventing the forgery and alteration of connection records<br>- encryption of personal information<br>- prevention of malicious programs<br>- preventing physical access<br>- protective measures in case of printing and copying<br>- protective measure by limiting the display of personal information<br>- protecting administrative terminals<br>- safety measures against disasters<br>- destroying personal information |
| | | (Addition) Are you applying the safety measure criteria according to personal information processor types and the amount of personal information?<br>Type 1) small businesses, organizations and individuals that have the personal information of less than 10,000 data subjects<br>Type 2) small and medium-sized businesses that have |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.<br><br>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.<br><br>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.<br><br>Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to | the personal information of less than 1 million data subject, large corporations, mid-sized companies and public institutions that have the personal information of less than 100,000 data subjects, and small businesses, organizations and individuals that have the personal information of 10,000 or more data subjects<br>Type 3) large corporations, mid-sized companies and public institutions that have the personal information of 100,000 or more data subjects, and small and medium-sized businesses and organizations that have 1 million or more data subjects |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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 proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held. | Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified.<br>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, | (Addition) Do you have and carry out the internal control plan which includes the details of technical, administrative and physical measures to protect personal information?<br>- providing education<br>- access control<br>- preventing the forgery and alteration of connection records<br>- encryption of personal information<br>- prevention of malicious programs<br>- preventing physical access<br>- protective measures in case of printing and copying<br>- protective measure by limiting the display of personal information<br>- protecting administrative terminals |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | use, alteration, disclosure, distribution, or access. | - safety measures against disasters<br>- destroying personal information |
| | | (Addition) Are you applying the safety measure criteria according to personal information processor types and the amount of personal information?<br>Type 1) small businesses, organizations and individuals that have the personal information of less than 10,000 data subjects<br>Type 2) small and medium-sized businesses that have the personal information of less than 1 million data subject, large corporations, mid-sized companies and public institutions that have the personal information of less than 100,000 data subjects, and small businesses, organizations and individuals that have the personal information of 10,000 or more data subjects<br>Type 3) large corporations, mid-sized companies and public institutions that have the personal information of 100,000 or more data subjects, and small and medium-sized businesses |
| 29. Describe how you make | The Accountability Agent must verify that the | 2.2.3.1 When hiring new employees, do you receive |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight). | 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:<br>• Training program for employees<br>• Regular staff meetings or other communications<br>• Security policy signed by employees<br>• Other (specify)<br>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 | information protection and personal information protection pledges which clearly state the responsibility for information protection and personal information protection? |
| | | 2.2.4.2 Do you regularly provide education at least once a year for all employees and outsiders within the scope of the management system according to the annual education plan, and provide additional education if there are important changes in related laws and regulations? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | this principle. | |
| 30. Have you implemented safeguards 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:<br><br>30.a) Employee training and management or other safeguards?<br><br>30.b) Information systems and management, including | Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards.<br><br>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.<br><br>Where the Applicant answers **NO** (to | (Addition) Do you have and carry out the internal control plan which includes the details of technical, administrative and physical measures to protect personal information?<br>- providing education<br>- access control<br>- preventing the forgery and alteration of connection records<br>- encryption of personal information<br>- prevention of malicious programs<br>- preventing physical access<br>- protective measures in case of printing and copying<br>- protective measure by limiting the display of personal |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| network and software design, as well as information processing, storage, transmission, and disposal?<br><br>30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?<br><br>30.d) Physical security? | 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. | information<br>- protecting administrative terminals<br>- safety measures against disasters<br>- destroying personal information |
| 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.<br><br>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. | 3.4.1.1 Do you establish internal policies related to the retention period and destruction of personal information? |
| | | 3.4.1.2 If the purpose of personal information processing is accomplished, or the retention period expires, do you immediately destroy the personal information? |
| | | 3.4.1.3 When you destroy personal information, do you destroy it in a way that ensures that it cannot be recovered or reproduced? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | | |
| 32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures? | | 2.9.5.1 Do you establish and implement the log review and monitoring procedure, including the log review cycle, targets and method to detect signs of abnormalities like information system-related errors, misuse and abuse (unauthorized connections, excessive access, etc.) and illegal behavior? |
| | 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.<br>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 | 2.9.5.2 Do you report the results of log review and monitoring to the responsible person, and take measures according to the procedure if signs of abnormalities are detected? |
| | | 2.11.2.1 Do you establish the procedure for inspecting information system vulnerabilities, and regularly inspect them? |
| | | 2.11.2.2 Do you take measures against detected vulnerabilities, and report the results to the responsible person? |
| | | 2.11.2.3 Do you continuously check if there are new security vulnerabilities, analyze impacts on the |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | | information system and take necessary measures? |
| | | 2.11.3.1 Do you collect such data as network traffic, data flow and event logs of key information systems, application programs, networks and security systems, and analyze and monitor them to detect abnormalities like internal and external infringement attempts, personal information leakage attempts and illegal behavior? |
| | | 2.11.3.2 Do you define the standards and thresholds for detecting infringement attempts, personal information leakage attempts and illegal behavior, and take timely follow-up measures, e.g. judgment and investigation of abnormalities? |
| 33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below. | 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. | 1.4.2.2 Do you have independent and objective manpower with expertise, perform inspections at least once a year according to the management system inspection plan, and report problems to the management? |
| | | 2.11.4.1 Do you establish the simulation training plan related to the procedure for responding to infringements |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | | and personal information leakage incidents, and periodically conduct simulation training at least once a year? |
| 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. | (Addition) Do you analyze and evaluate the vulnerabilities related to personal information protection, e.g. certifications related to personal information protection (PIMS, ISMS, personal information impact assessment and ISO27001) and key information and communications infrastructure? |
| | | (Addition) Do you have and carry out the internal control plan which includes the details of technical, administrative and physical measures to protect personal information?<br>- providing education<br>- access control<br>- preventing the forgery and alteration of connection records<br>- encryption of personal information<br>- prevention of malicious programs<br>- preventing physical access |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | | - protective measures in case of printing and copying<br>- protective measure by limiting the display of personal information<br>- protecting administrative terminals<br>- safety measures against disasters<br>- destroying personal information |
| 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:<br>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. | 2.3.2.2 Do you identify information protection and personal information protection requirements due to the use of external services and the outsourcing of business, and specify them in the contract or agreement? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| sensitivity of the information and services provided?<br><br>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?<br><br>35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach? | | |
| | | 2.3.3.1 Do you periodically inspect or audit whether outsiders are complying with the information protection and personal information protection requirements, specified in the contract, agreement and internal policies? |
| | | 2.3.3.2 Do you establish and implement improvement plans with regard to the problems found during inspection or audit of outsiders? |

**ACCESS AND CORRECTION**

**Assessment Purpose -** *The questions in this are directed towards ensuring that individuals are able to access and correct their information. This 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. 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*)** | **Program Requirement of KISA** |
|---|---|---|
| 36. Upon request, do you provide confirmation of whether or not you hold personal | Where the Applicant answers **YES**, the Accountability Agent must verify that the | 3.5.2.2 If the information subject (user) or his/her agent requests access to personal information, do you take necessary measures so that it is possible to access the |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| information about the requesting individual? Describe below. | Applicant has procedures in place to respond to such requests.<br><br>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.<br><br>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.<br><br>The personal information must be provided to individuals in an easily comprehensible way.<br><br>The Applicant must provide the individual with a time frame indicating when the requested access will be granted.<br><br>Where the Applicant answers **NO** and does not identify an applicable qualification, the | personal information within the prescribed period? |
| | | 3.1.5.4 If the information subject (user) requests it when personal information is collected from someone other than the information subject (user), do you immediately notify necessary matters to the information subject (user)? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | 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. | |
| 37. Upon request, do you provide individuals access to the personal information that you hold about them?<br>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. | Where the Applicant answers **YES** the Accountability Agent must verify each answer provided.<br>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.<br>If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the | 3.5.2.1 Do you have the method and procedure for exercising rights so that the information subject (user) or his/her agent can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw consent (hereinafter referred to as 'access, etc.') more easily than the personal information collection method and procedure? |
| | | (Addition) If access to personal information is requested, is there a procedure for self-authentication? (PIMS 6.1.1.3) |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.<br><br>37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe.<br><br>37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.<br><br>37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual | appropriate contact information for challenging the denial of access where appropriate.<br><br>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. | 3.5.2.2 If the information subject (user) or his/her agent requests access to personal information, do you take necessary measures so that it is possible to access the personal information within the prescribed period? |
| | | (Addition) If the information subject (user) or his/her agent requests access to personal information, do you provide the information provided in a form that can be easily understood by the information subject? |
| | | (Addition) If the information subject (user) or his/her agent requests access to personal information, do you provide methods that the information subject can easily use, e.g. in writing, by phone, e-mail and Internet? |
| | | (Addition) Do you demand fees for the request to access personal information within the necessary range of actual expenses? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| (e.g. email, same language, etc)?<br><br>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. | | |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | | |
| 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).<br><br>38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space | 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.<br><br>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.<br><br>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 | 3.5.2.1 Do you have the method and procedure for exercising rights so that the information subject (user) or his/her agent can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw consent (hereinafter referred to as 'access, etc.') more easily than the personal information collection method and procedure? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| below or in an attachment if necessary.<br><br>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?<br><br>38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?<br><br>38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that | 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.<br><br>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. | 3.5.2.3 If the information subject (user) or his/her agent requests correction or deletion of personal information, do you take necessary measures so that it is possible to correct or delete the personal information within the prescribed period? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| the data has been corrected or deleted?<br><br>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? | | 3.5.2.5 If the information subject (user) objects to the measures taken with regard to his/her request, do you have necessary procedures for their raising an objection, and provide information on it? |

**ACCOUNTABILITY**

**Assessment Purpose -** *The questions in this 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*)** | **Program Requirement of KISA** |
|---|---|---|
| 39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe.<br>• Internal guidelines or policies (if applicable, | The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles. | 1.4.1.1 Do you identify the legal requirements related to information protection and personal information protection that the organization must comply with, and keep them up-to-date? |
| | | 2.1.1.2 When there is an important change in the environment in and outside of the organization, do you review its influence on the policies and implementation documents related to information protection and personal information protection, and revise them if necessary? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| describe how implemented) _____<br>• Contracts _____<br>• Compliance with applicable industry or sector laws and regulations ____<br>• Compliance with self-regulatory applicant code and/or rules ____<br><br>Other (describe) ____ | | |
| 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 | 1.1.2.1 Does the CEO officially appoint the chief information security officer and the chief privacy officer who supervise information protection and personal information protection? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | is responsible for the Applicant's overall compliance with these Principles.<br><br>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.<br><br>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. | |
| 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, | 3.5.2.1 Do you have the method and procedure for exercising rights so that the information subject (user) or his/her agent can access, correct or delete personal information, suspend the processing thereof, raising |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | investigate and respond to privacy-related complaints, such as:<br>1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR<br>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<br>3) A formal complaint-resolution process; AND/OR<br>4) Other (must specify).<br>Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such | objections, and withdraw consent (hereinafter referred to as 'access, etc.') more easily than the personal information collection method and procedure? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | procedures is required for compliance with this principle. | |
| 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.<br>Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle. | 3.5.2.2 If the information subject (user) or his/her agent requests access to personal information, do you take necessary measures so that it is possible to access the personal information within the prescribed period? |
| | | 3.5.2.3 If the information subject (user) or his/her agent requests correction or deletion of personal information, do you take necessary measures so that it is possible to correct or delete the personal information within the prescribed period? |
| 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. | 3.5.2.2 If the information subject (user) or his/her agent requests access to personal information, do you take necessary measures so that it is possible to access the personal information within the prescribed period? |
| | | 3.5.2.3 If the information subject (user) or his/her agent |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| | | requests correction or deletion of personal information, do you take necessary measures so that it is possible to correct or delete the personal information within the prescribed period? |
| 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.<br>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. | 2.2.4.4 Do the employees in the IT and information protection, personal information protection organization receive separate education for enhancing expertise of each job in relation to information protection and personal information protection? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| 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.<br>Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle. | (Addition) If you are dealing with the government, do you have and follow the procedure for conducting this business? |
| 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 | Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described.<br>Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such | 2.3.2.1 'If you select external services and outsourcees in relation to important information and personal information processing, do you have procedures for taking information protection and personal information protection competency into consideration? |
| | | 2.3.2.2 Do you identify information protection and personal information protection requirements due to the |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| ensure that your obligations to the individual will be met (check all that apply)?<br>• Internal guidelines or policies _____<br>• Contracts _____<br>• Compliance with applicable industry or sector laws and regulations _____<br>• Compliance with self-regulatory applicant code and/or rules _____<br>Other (describe) _____ | agreements is required for compliance with this principle. | use of external services and the outsourcing of business, and specify them in the contract or agreement? |
| 47. Do these agreements | The Accountability Agent must verify that the | 2.3.2.2 Do you establish and implement improvement plans with regard to the problems found during |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| generally require that personal information processors, agents, contractors or other service providers:<br>• Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement?_____<br>• Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement?_____<br>• Follow instructions provided by you relating to the manner in which your personal information must be handled?_____ | Applicant makes use of appropriate methods to ensure their obligations are met. | inspection or audit of outsiders? |
| | | 2.3.3.3 'If the outsourcee, whom personal information processing is outsourced to, re-outsources the business to a third party, do you make sure that it is approved by |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| • Impose restrictions on subcontracting unless with your consent? _____<br>• Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____<br>• Notify the Applicant in the case of a breach of the personal information of the Applicant's customers?<br>Other (describe) _____ | | the outsourcer? |
| 48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure | The Accountability Agent must verify the existence of such self-assessments. | 2.3.3.1 Do you periodically inspect or audit whether outsiders are complying with the information protection and personal information protection requirements, specified in the contract, agreement and internal policies? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| compliance with your instructions and/or agreements/contracts? If YES, describe below | | |
| 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.<br>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. | 2.3.3.1 Do you periodically inspect or audit whether outsiders are complying with the information protection and personal information protection requirements, specified in the contract, agreement and internal policies? |
| 50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence | If **YES**, the Accountability Agent must ask the Applicant to explain:<br>(1) why due diligence and reasonable steps consistent with the above Assessment Criteria | (Addition) If personal information is disclosed to a third party who is difficult to manage or supervise, how the security measures are required? |

| **Question (*to be answered by the Applicant Organization*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Program Requirement of KISA** |
|---|---|---|
| and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible? | for accountable transfers are impractical or impossible to perform; and<br>(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. | |