APEC CBPR Accountability Agent Renewal Application

1. In regards to APEC CROSS BORDER PRIVACY RULES SYSTEM (hereinafter referred to as 'CBPR'), we, Korea Internet & Security Agency(hereinafter referred to as 'KISA'), are pleased to re-apply for the Accountability Agent.

2. KISA is a special corporation(a generic name for corporations established by national policy according to special laws for public interests) established in accordance with the 'Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.', and a public institution pursuant to the 'Act on the Management of Public Institutions'. Under these laws, KISA's all activities including those related to personal information protection or activities as an APEC CBPR Accountability Agent or any other, should be managed and supervised by the competent authorities such as the Ministry of Science and ICT and Personal Information Protection Commission.

<Relavant laws and regulation>

1) *The Regulation on Delegation and Entrustment of Administrative Authorities*

When the administrative institution delegates a part of its power or authority, or entrust a part of its tasks provided to the related law, to the subsidiary institution or corporate, etc, then the delegated or entrusted institution shall comply the applicable law and carry out tasks faithfully(Article 5). The competent authority is entitled to conduct and supervise the delegated or entrusted institution for the tasks, and suspend or revoke it when illegal or unfair process is found(Article 6, Article 14).

2) *Act on the Management of Public Institutions*

The public institution such as 'an institution directly established pursuant to other Act with an investment by the government', is obliged to publish the management performance and annual report, etc.(Article 4, Article 11, Article 47, Article 49). The Chief of the competent administrative institution is empowered to supervise performance of the public institution(Article 51).

3) *The ICT Network Act*

The Government shall establish KISA in order to promote the safe use of the information and communications network, etc and KISA shall perform business affairs including research and development of measures & technology for personal information protection pursuant to the Personal Information Protection Act(PIPA).

4) *Personal Information Protection Act(PIPA)*

PIPC shall perform business affairs including tasks on establishing and executing policies, cooperating with overseas authorities or international bodies as well as investigating on infringement of data subject right(Article 7-8). Pursuant to PIPA, PIPC entrusts KISA with a power of education on personal information protection, investigation on complaint, etc(Article 68).

3. Also, KISA confirms that the documents necessary for the APEC CBPR Accountability Agent application and additional documents are provided in the form of annexes or appendixes as follows.

1) APEC CBPR Accountability Agent Recognition Criteria Checklist (Annex A)
2) APEC CBPR PROGRAM REQUIREMENTS MAP (Annex B)
3) Signature and Contact Information (Annex C)
4) KISA's Guideline for APEC CBPR certification (Appendix 1)

※ Since KISA has not received any complaints from the public to the certified companies, it submits the application documents for renewal except in Annex D(Case Notes) and Annex E(Complaint Statistics), If we receives any complaints, we will make publicly available information on the number of complaints and dispute resolution outcomes of complaints and release case notes on a selection of essential complaints.

4. I appreciated all your efforts in reviewing the documents and proceeding forward steps. If you have any questions, please contact Taein Jung, manager of the Personal Data Cooperation Team(tijung@kisa.or.kr).

Eun-A Na
Director of the Personal Data Policy Division at KISA

Annex A

APEC CBPR Accountability Agent Recognition Criteria Checklist

1 Conflict of Interest

Criteria	Operating status of KISA
1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.	◎ Korea Internet & Security Agency(hereinafter KISA) is a special organization established by national policy according to special laws the 'Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.(hereinafter Network Act) for the public interest, and as a public agency under the 'Act on the Management of Public Institutions', KISA performs its duties fairly and objectively under the management and supervision of the Ministry of Science and ICT(MSICT), and Personal Information Protection Commission(hereinafter PIPC) etc. Specifically, Paragraph 1 of Article 52 of the Network Act stipulate the purpose of establishing KISA. ◎ KISA is a nonprofit special organization established for public interests in national policies, and performs duties based on fairness and objectivity under the management and supervision of the competent PEA, the PIPC. Accordingly, unlike associations and organizations which are run based on the membership fee, or private enterprises whose

Criteria	Operating status of KISA
	main purpose is to create profits, KISA runs on government budgets, and the revenues from certification activities are also used for national budget or public purposes. So it can perform certification activities fairly without any interest in certain institutions or business operators. ※ 「**Network Act**」 **Article 52 (Korea Internet & Security Agency)** ① The Government shall establish the KISA to upgrade the information and communications network (excluding matters concerning establishment, improvement and management of information and telecommunications network), encourage the safe use thereof, and promote the international cooperation and advancement into the overseas market in relation to broadcasting and communications.
2. Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b)* of Annex A.	◎ KISA is a public institution that performs public affairs, and is under the supervision and management of the relevant government bodies. According to the 'Improper Solicitation and Graft Act' and other policies of government, KISA is establishing and operating internal regulations such as 「Code of Conduct for Employees」 and regular integrity training sessions for employees` fair performances. ◎ For example, according to Articles 5 and 7 of the 「Code of Conduct for Employees」 of KISA, if the duties employees perform are directly related to themselves, their families, the organizations they worked for in the past, or the representatives of such organizations, or people who are deemed to have difficulty performing their duties

Criteria	Operating status of KISA
	fairly, e.g. people who had financial transactions in excess of a certain amount, KISA must take measures, such as reassignment of duties or manpower. This code of conduct applies to all KISA employees according to Article 3 (Scope of application). ※ **KISA Code of Conduct for Employees** Article 3 (Scope of application) This code of conduct applies to all employees of KISA. ※ **KISA Code of Conduct for Employees** Article 5 (Reporting private interests, etc.) ① If employees fall under any of the following cases … they should report it to their superiors or the president of Korea Internet & Security Agency. 1. If employees themselves are persons related to their duties; 2. If the relatives of employees closer than cousins are persons related to their duties; 3. If the corporation and organization for which employees themselves worked in the past 2 years are persons related to their duties; 4. If the corporation and organization in which employees themselves or their families are employees or outside directors are persons related to their duties; and … 7. If persons who the president of KISA said are difficult to perform duties fairly are persons related to their duties. ② KISA may request such measures as reassignment of duties for persons related to their duties or persons who have an interest in the duties performed by employees. ④ The president of KISA, who receive the report pursuant to Paragraph 1 or the application pursuant to Paragraphs 2 and 3 may take any of the following measures against such employees if it is deemed to hinder their fair performance of duties.

Criteria	Operating status of KISA
	1. Temporary suspension of participation in duties 2. Designation of a person acting on their behalf or a person who perform duties jointly 3. Reassignment of duties 4. Transfer ※ **KISA Code of Conduct for Employees** Article 7 (Prohibition of profit-making activities related to duties) ① Employees may not do any of the following in relation to the duties of KISA: 1. Privately providing labor, advice or consulting to persons related to their duties and getting paid 2. Representing the counterpart of the agency they belong to or providing advice, consulting or information to the counterpart if they perform duties which involve the agency they belong to in a dispute, or the duties they perform have a direct interest in the agency they belong to ⋮ 5. Behavior related to the duties that the president of KISA deems likely to hinger the fair and disinterested performance of duties ② If the behavior of employees is deemed to fall under any of the following in Paragraph 1, the president of KISA must stop the behavior or order them to terminate it. ◎ Meanwhile, KISA stipulates the roles and duties of the certification committee and certification auditors through the 「Guideline for APEC CBPR Certification」 (hereinafter, Guideline). Paragraph 4 of Article 12 specifies cases in which certification auditors should be excluded, as those who have participated in the applicants in last 3 years or have experiences in security consulting related work of the

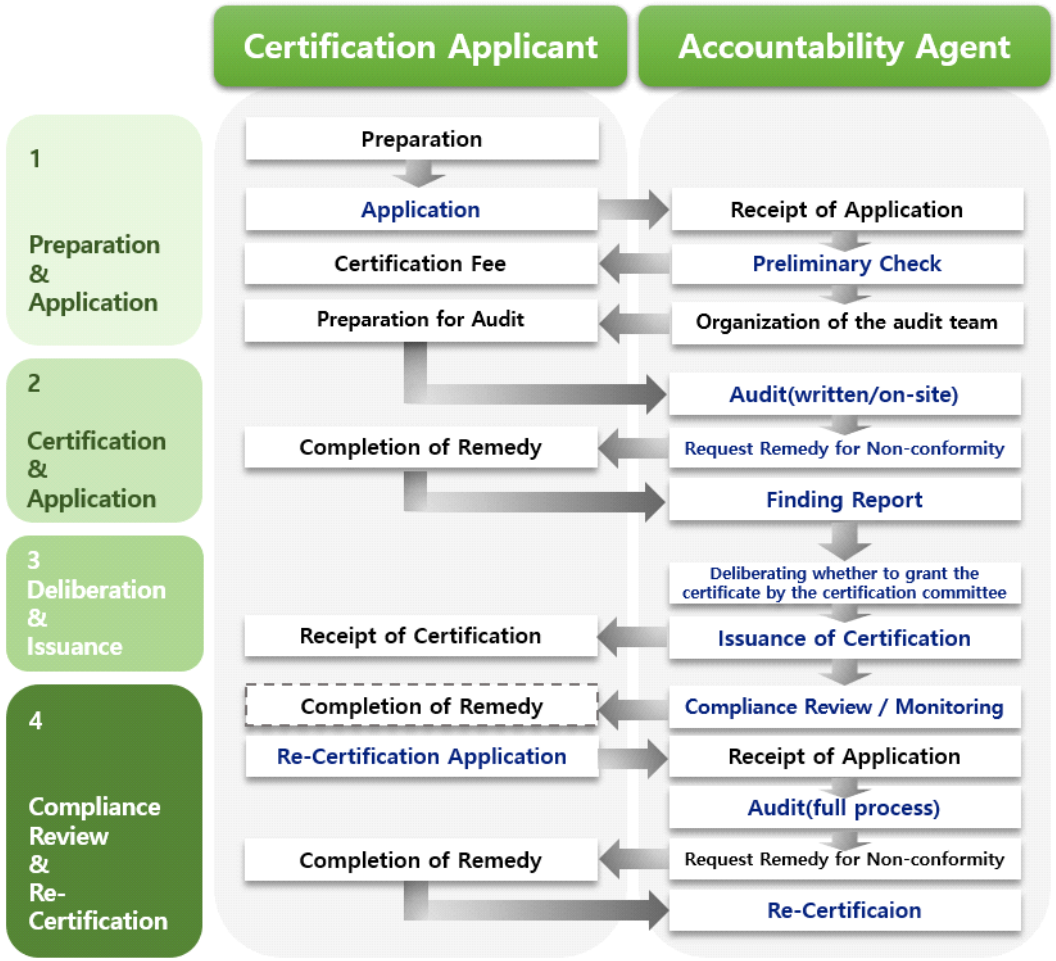
Criteria	Operating status of KISA
	applicants in last 3 years, or have any interest with the applicants, are excluded from the certification assessment team. ◎ Also, KISA is preventing various conflicts of interest likely to occur in the process of performing certification and securing independence, fairness, and reliability as a CBPR accountability agent, by stipulating the cases which can exclude, avoid, and evade the certification committee members who have interests with the deliberation agendas, through the Article 9 of the guideline. ※ **Guideline for APEC CBPR Certification** Article 9 (Exclusion, avoidance and evasion) ① Committee members are excluded from deliberation and decision of the agenda if the agenda of the committee falls under any of the following subparagraphs: 1. Matters of direct interest to committee members themselves 2. Matters related to persons who are or were relatives of the committee members themselves; 3. Matters of direct interest to committee members themselves due to special legal relationship, etc.; and 4. Matters whose audit/investigation or inspection they were involved in before becoming committee members ※ **Guideline for APEC CBPR Certification** Article 12 (Organization of the certification audit team) ④ When the certification audit team is organized, the following certification auditors must be excluded: 1. Auditors who are affiliated with the applicant or have been affiliated with the applicant for the past three years

Criteria	Operating status of KISA
	2. Auditors who have performed related tasks, e.g. security consulting and outsourced work, for the applicant in the past three years 3. Auditors who have a relationship with the applicant pursuant to Paragraph 1 of Article 9
3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.	◎ In accordance with Article 5 of the Rules, the President of KISA may dismiss the committee members when they violate these rules or laws, so that KISA is actually preventing conflicts of interests. ※ **Guideline for APEC CBPR Certification** Article 5 (Excluding committee members and selecting substitute committee members) ① The president of KISA excludes committee members from the committee when they violate laws or this guideline. <Amended on September 28, 2022> ② If there is a vacancy in the committee for the following reasons, a substitute committee member may be appointed. 1. If it was confirmed that a committee member received bribes, solicited favors from interested parties or exerted undue influence in the course of the committee's activities, and he or she was excluded from the committee; and <Amended on September 28, 2022>

2 Program Requirements

Criteria	Operating status of KISA
4. Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.	◎ KISA is mapping the detailed assessment criteria based on the existing domestic certification system, 'Personal Information & Information Security Management System(ISMS-P) to APEC's 50 CBPR program requirements as shown in <Annex B> to satisfy APEC's criteria.

3 Certification Process

Criteria	Operating status of KISA
5. Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d)* of Annex A have been met.	◎ KISA's APEC CBPR operating system includes the following certification process. 

4 On-going Monitoring and Compliance Review Processes

Criteria	Operating status of KISA
6. Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).	◎ KISA's certification procedures include preliminary check and on-site inspection in addition to the self-assessment, and document review to make sure of the readiness of the applicant and trustable assessment. With the preliminary check, the applicant can be sure that if their information system, procedure is ready for the assessment. Moreover, on-site inspection helps to verify the applicant's self-assessment, making it possible for assessors to access to the internal documents or the information systems, and other relevant equipment which cannot, or should not be disclosed to the outside of applicant. ◎ Above all, KISA operates certification committee for the further fairness of assessment. The committee is a independent organization deliberating the findings report of assessment team, and make a decision on issuance of certificate. ◎ To check the participant to adhere to the CBPR, KISA keeps monitoring participants indirectly such as monitoring the relevant media, complaint etc. ◎ KISA stipulates these audit procedures in the Guideline and Manual with detailed. ※ **Guideline for APEC CBPR Certification** Article 11 (Preliminary check) ① KISA can conduct a written or on-site inspection of the applicant's preparation for audit. ② If KISA cannot conduct a certification audit due to insufficient preparation of the applicant, KISA

	may request supplementary measures and postpone the certification audit. ※ **Guideline for APEC CBPR Certification** Article 16 (Certification audit) ① The certification audit combines document-based and on-site audit of applicants. ② In the document-based audit, administrative elements are audited for compliance with [Appendix 1] by reviewing the privacy policy and evidence of policy implementation. ③ In the on-site audit, technical elements are audited by interviewing the person in charge, checking related systems, and checking vulnerabilities in order to check the results of the document-based audit and whether technical and physical protection measures have been implemented. ④ KISA prepares a [Appendix 8] defect report for problems found in the certification audit, and prepares a [Appendix 9] request for supplementary measures for defects, and requests supplementary measures from the applicant. ⑤ <Deleted on September 28, 2022> ※ **Guideline for APEC CBPR Certification** Article 17 (Supplementary measures) ① The applicant must take the supplementary measures within 40 days from the date of receiving the request for supplementary measures, fill out the supplementary measures statement in [Appendix 11], and submit it to KISA along with an official document on the completion of the supplementary measures. ② If supplementary measures are not completed within 40 days, the applicant should prepare [Appendix 11] supplementary measures statement for defects for which supplementary measures are completed, and [Appendix 12] supplementary measures summary for defects for which supplementary measures are not completed, and submit an official notice of extension of the supplementary measures. In this case, the audit team leader can additionally grant a supplementary measures period of up to 60 days if it is judged that the reason for extending the supplementary measures is justifiable. ③ The audit team leader can visit the site and check the results if on-site confirmation of the details of

	the supplementary measures submitted by the applicant is deemed to be necessary. ④ Completion of supplementary measures in Paragraph 2 refers to the completion of the supplementary measures completion confirmation in [Appendix 13] including signatures of the applicant's privacy officer and audit team leader. <Amended on September 28, 2022> ※ **Guideline for APEC CBPR Certification** Article 20 (Issuance of certificates, etc.) ① The president of KISA notifies the applicant of the result when the result of deliberation/decision by the committee is submitted, and if the applicant is judged to meet the APEC CBPR certification criteria in [Appendix 1], the APEC CBPR certificate in [Appendix 4] must be issued. ② The certificate is valid for one year according to Paragraph 1. ③ If KISA deems it necessary, e.g. the occurrence of serious personal information protection incidents for those who have obtained the certification or the filing of complaints in accordance with Paragraph 2 of Article 25, the president of KISA may request the organization that has obtained the certification to submit separate data within the scope of the certification. ◎ Meanwhile, Article 20 of the Guideline stipulates matters related to monitoring of certified institutions. When a serious personal information infringement accident occurs or a complaint is received by the certified companies, KISA may request submission of materials, etc. according to KISA`s determination, and KISA could execute checking the website security, inspecting vulnerability, and technical inspection for vulnerability remotely, etc. ◎ In addition, the Guidelines stipulate the follow-up management of certificates (Article 23, Article 25) to monitor participants' compliance continuously. In addition, when issuing

	certificates to the participants, the self-regulation obligations of participants are strengthened by attaching a confirmation of compliance with the program requirements. ※ **Guideline for APEC CBPR Certification** Article 23 (Cancellation of certification) ① KISA may cancel certification through deliberation and decision of the committee when it finds any of the following reasons: 1. If certification has been obtained by false or fraudulent means or the organization that has obtained certification fails to comply with it afterwards; 2. If an organization that has obtained certification falsely publicizes details of the certification; and 3. If an organization that has obtained certification does not take necessary measures to handle personal information complaints in accordance with Paragraph 4 of Article 25 ② When KISA cancels certification in accordance with Paragraph 1, it must notify the organization that has obtained the certification, take back the issued certificate, and disclose the fact. ※ **Guideline for APEC CBPR Certification** Article 25 (Handling complaints related to personal information, etc.) ① Anyone who finds an organization that has obtained certification does not comply with APEC CBPR certification can file a complaint with KISA. ② Upon receipt of the complaint, KISA examines whether the reported matter falls within the APEC CBPR compliance scope of the organization that has obtained the certification, and if so, may request the organization that has obtained the certification to confirm the fact and make corrections. ③ If KISA needs to provide the personal information of the person who filed the complaint to a third party while handling the complaint, it must obtain prior consent from him or her. ④ An organization that has obtained certification must take corrective action within 30 days from the date of receiving the request for corrective action, and submit an official document and corrective action details to KISA in writing.

	⑤ If an organization that has obtained certification needs to have the corrective action period extended, he or she must submit an official document about the extension and a written corrective action plan to KISA within 30 days. If KISA determines that the reason for the extension is justified, it may grant an additional 30-day corrective action period. ⑥ KISA notifies the receipt of the complaint and the result of handling the complaint to the person who filed the complaint and the organization that has obtained certification in writing or electronically. ⑦ KISA regularly discloses APEC CBPR complaint handling statistics and anonymized casebooks.
7. Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.	◎ In accordance with the Guideline, KISA may suspend the assessment if the applicant is not cooperative with the assessment procedures. Also, if a company acquired the certificate by fraudulent methods or the supplementary measures are not implemented, the certificate could be canceled. ※ **Guideline for APEC CBPR Certification** Article 19 (Suspension of audit) ① Where the applicant intentionally delays or obstructs the implementation of the certification audit or where it is deemed difficult to proceed with the certification audit due to reasons attributable to the applicant; 2. When it is believed that the applicant is not ready for certification after reviewing the relevant data submitted by the applicant; 3. If supplementary measures in accordance with Article 17 are not completed after the certification audit; 4. If it is judged that the certification audit is impossible due to natural disasters or changes in the business environment, etc. ② If the certification audit is suspended, the applicant must prepare the certification audit suspension confirmation in [Appendix 10] and submit it to KISA. ③ KISA may resume or terminate the certification audit if the reasons for suspension of the certification audit in Paragraph 1 are resolved, or according to the result of processing the objection

	pursuant to Article 24. ※ **Guideline for APEC CBPR Certification** Article 23 (Cancellation of certification) ① KISA may cancel certification through deliberation and decision of the committee when it finds any of the following reasons: 1. If certification has been obtained by false or fraudulent means or the organization that has obtained certification fails to comply with it afterwards; 2. If an organization that has obtained certification falsely publicizes details of the certification; and 3. If an organization that has obtained certification does not take necessary measures to handle personal information complaints in accordance with Paragraph 4 of Article 25 ② When KISA cancels certification in accordance with Paragraph 1, it must notify the organization that has obtained the certification, take back the issued certificate, and disclose the fact.

5 Re-Certification and Annual Attestation

Criteria	Operating status of KISA
8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d)* of Annex A.	◎ Participants must apply for re-certification by 3 months before expiration of the term of validity of certification according to Article 22 of the Guideline. Re-certification criteria and procedures will comply with the program requirements and procedures described in recognition criterion 5, and if the term of validity of certification expires without applying for re-certification, issued certification will lose effect. ※ **Guideline for APEC CBPR Certification** Article 22 (Re-certification audit) ① If an organization that has obtained certification wants to extend the validity of the certificate, he or she must apply for a re-certification audit three months before the validity period of the certificate expires. ② The re-certification audit is conducted in accordance with Chapter 4(Certification Audit).

6 Dispute Resolution Process

Criteria	Operating status of KISA
9. Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate. 10. Applicant Accountability Agent should describe how the dispute resolution process meets the requirements identified in 10 (a) – (h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third-party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A)	◎ In accordance with Article 25 of the Guideline, anyone can raise complaints to KISA when a complaint related to CBPR certification occurs. If the report of the civil petitioner is within the CBPR compliance scope of the certified organization, KISA will notify the reception of the civil complaint to the civil petitioner in wiring or electronic document and check the facts. Based on the result of investigation, KISA may request the participants to take corrective measures in regard to inadequacies, and if it fails to do so, it may cancel certification. Also, KISA offers the guides information on CBPR participants and how to raise questions about matters that do not meet the CBPR certification criteria of participants through the CBPR certification web-page. ※ **Guideline for APEC CBPR Certification** Article 25 (Handling complaints related to personal information, etc.) ① Anyone who finds an organization that has obtained certification does not comply with APEC CBPR certification can file a complaint with KISA. ② Upon receipt of the complaint, KISA examines whether the reported matter falls within the APEC CBPR compliance scope of the organization that has obtained the certification, and if so, may request the organization that has obtained the certification to confirm the fact and make corrections. ③ If KISA needs to provide the personal information of the person who filed the complaint to a third party while handling the complaint, it must obtain prior consent from him or her. ④ An organization that has obtained certification must take corrective action within 30 days from the

as well as its process to submit the required information in Annexes D and E.	date of receiving the request for corrective action, and submit an official document and corrective action details to KISA in writing. ⑤ If an organization that has obtained certification needs to have the corrective action period extended, he or she must submit an official document about the extension and a written corrective action plan to KISA within 30 days. If KISA determines that the reason for the extension is justified, it may grant an additional 30-day corrective action period. ⑥ KISA notifies the receipt of the complaint and the result of handling the complaint to the person who filed the complaint and the organization that has obtained certification in writing or electronically. ⑦ KISA regularly discloses APEC CBPR complaint handling statistics and anonymized casebooks. ◎ In the event of receiving complaints, KISA plan to publish related dispute resolution case notes and complaints statistics. There have been no civil complaints since the CBPR system's launch. ◎ KISA also is planning to cooperate with overseas law enforcement authorities or accountability agents, which joined CBPR for the sake of handling civil complaints or cooperation in law enforcement according to Article 26 of the Guideline. ※ **Guideline for APEC CBPR Certification** Article 26 (International Cooperation) KISA cooperates with foreign law enforcement agencies or APEC CBPR accountability agents in relation to APEC CBPR certification to handle civil complaints and cooperate with law enforcement.

7 Mechanism for Enforcing Program Requirements

Criteria	Operating status of KISA
11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.	◎ KISA has secured practical enforcement authority for certification applicants and certified companies by establishing regulations in the Rules to suspend certification examination or cancel issued certification. ◎ In accordance with Article 19 of the Rules, KISA stipulates that the certification assessment could be stopped if the applicant`s program requirements are not met. In addition, according to the Article 23 of the Rules, the certification may be canceled if the certified company acquired certification by fraudulent methods or falsely promoted the contents of the certification, or did not take corrective measures for the reported complaint. At this time, KISA retrieves the issued certification and discloses the fact through its CBPR website. ※ **Guideline for APEC CBPR Certification** Article 19 (Suspension of audit) ① Where the applicant intentionally delays or obstructs the implementation of the certification audit or where it is deemed difficult to proceed with the certification audit due to reasons attributable to the applicant; 2. When it is believed that the applicant is not ready for certification after reviewing the relevant data submitted by the applicant; 3. If supplementary measures in accordance with Article 17 are not completed after the certification audit; 4. If it is judged that the certification audit is impossible due to natural disasters or changes in the business environment, etc.

	※ **Guideline for APEC CBPR Certification** Article 23 (Cancellation of certification) ① KISA may cancel certification through deliberation and decision of the committee when it finds any of the following reasons: 1. If certification has been obtained by false or fraudulent means or the organization that has obtained certification fails to comply with it afterwards; 2. If an organization that has obtained certification falsely publicizes details of the certification; and 3. If an organization that has obtained certification does not take necessary measures to handle personal information complaints in accordance with Paragraph 4 of Article 25 ② When KISA cancels certification in accordance with Paragraph 1, it must notify the organization that has obtained the certification, take back the issued certificate, and disclose the fact. ◎ The Articles on the suspension of assessment and cancellation of certification are applied through the entire certification application and maintenance process between KISA and the company, and have the same effect as the contract between the two parties. Therefore, KISA is securing the executive authority based on the contractual effect of the certification body.
12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to	◎ As discussed in the accountability agent checklist 10 and 11, KISA notify non-compliance of the participant in accordance with Article 23 and 25, and may impose penalties regarding it. ◎ If it is confirmed that the participant does not comply with the CBPR requirements, KISA may request corrective measures on it, and if those measures are not

ensure the participant remedy the non-compliance. 13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e)* of Annex A.	implemented within the specified time limit, the certification may be canceled according to the deliberation and decision of the certification committee. If the certified company has objections to this determination, it can raise an objection within 15 days from the date of notification of the result. ※ **Guideline for APEC CBPR Certification** Article 23 (Cancellation of certification) ① KISA may cancel certification through deliberation and decision of the committee when it finds any of the following reasons: 1. If certification has been obtained by false or fraudulent means or the organization that has obtained certification fails to comply with it afterwards; 2. If an organization that has obtained certification falsely publicizes details of the certification; and 3. If an organization that has obtained certification does not take necessary measures to handle personal information complaints in accordance with Paragraph 4 of Article 25 ② When KISA cancels certification in accordance with Paragraph 1, it must notify the organization that has obtained the certification, take back the issued certificate, and disclose the fact. ※ **Guideline for APEC CBPR Certification** Article 24 (Objection) ① An applicant or an organization that has obtained certification may file an objection within 15 days when notified by KISA of the deliberation result regarding certification suspension or cancellation. At this time, the organization concerned must submit the objection statement in [Appendix 7] to KISA. ② KISA may request the committee to deliberate if the objection pursuant to Paragraph 1 is deemed reasonable. ③ KISA must notify the result of handling the objection to the organization that filed the objection in writing.

	※ **Guideline for APEC CBPR Certification** Article 25 (Handling complaints related to personal information, etc.) ① Anyone who finds an organization that has obtained certification does not comply with APEC CBPR certification can file a complaint with KISA. ② Upon receipt of the complaint, KISA examines whether the reported matter falls within the APEC CBPR compliance scope of the organization that has obtained the certification, and if so, may request the organization that has obtained the certification to confirm the fact and make corrections. ③ If KISA needs to provide the personal information of the person who filed the complaint to a third party while handling the complaint, it must obtain prior consent from him or her. ④ An organization that has obtained certification must take corrective action within 30 days from the date of receiving the request for corrective action, and submit an official document and corrective action details to KISA in writing. ⑤ If an organization that has obtained certification needs to have the corrective action period extended, he or she must submit an official document about the extension and a written corrective action plan to KISA within 30 days. If KISA determines that the reason for the extension is justified, it may grant an additional 30-day corrective action period. ⑥ KISA notifies the receipt of the complaint and the result of handling the complaint to the person who filed the complaint and the organization that has obtained certification in writing or electronically. ⑦ KISA regularly discloses APEC CBPR complaint handling statistics and anonymized casebooks.
14. Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law	◎ The Personal Information Protection Commission(hereinafter 'PIPC') is an enforcement authority of Personal Information Protection Act(hereinafter 'PIPA') which joined CBPR, and KISA is a public organization that supports affairs such as research on personal information protection policies and technology dissemination of the PIPC(refer to the checklist 1). In general, non-compliance with the CBPR requirements is a

enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].	violation of PIPA, and KISA promptly notify and discuss about serious violations through a constant cooperation system with PIPC. ◎ In addition, KISA has established 「Rules for handling complaints and reports」 in order to determined details necessary for handling received complaints, and Paragraph 1 of Article 4 of thess rules stipulate cases in which received complaints can be transferred to other organizations so that more sufficient handling on complaints is possible. ※ **Rules for handling complaints and reports** Article 4 (Principles of handling) ① In principle, KISA shall handle complaints received by itself. However, if it falls under any of the following, it may be transferred to other organizations. 1. When it is determined that the content of received complaint is not under the responsibility of KISA 2. When it is deemed appropriate to be handled by related other organizations 3. When it is determined that transferring to other organization is more helpful to a civil petitioner
15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.	◎ As discussed in the accountability agent checklist 9, KISA is establishing cooperative system for handling the civil complaint with enforcement authorities of APEC member economies and CBPR accountability agents. In addition, through a cooperative system with PIPC which is a member organization of APEC CPEA, KISA is maintaining the responding system for CBPR related complaints within APEC. ※ **Guideline for APEC CBPR Certification** Article 26 (International Cooperation) KISA cooperates with foreign law enforcement agencies or APEC CBPR accountability agents in relation to APEC CBPR certification to handle civil complaints and cooperate with law enforcement.

Annex B

KISA 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 checklists

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: • 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).	3.5.1 You must establish the personal information processing policy, including all necessary matters like the purpose of processing personal information, and disclose it and continuously update it in such a way that the data subject (user) can always check it easily.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria** (*to be verified by the Accountability Agent*)	**Program Requirement of KISA**
	• Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. States an effective date of Privacy Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must	

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.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: ☐ The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. ☐ the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and ☐ The Privacy Statement reports the categories or specific sources of all categories of personal information collected.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria** (*to be verified by the Accountability Agent*)	**Program Requirement of KISA**
	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. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the	

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

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: ☐ The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). ☐ The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests,	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	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.	
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives. 3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	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.	protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.
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. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives. 3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	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.	protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives. 3.3.1 If personal information is provided to a third

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	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.	party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.

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: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	1.2.2 You must analyze the current status of information service and personal information processing with regard to all areas of the management system, identify and document the business procedure and flow, periodically review them and keep them up-to-date.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. Using the above, the Accountability Agent will verify that the applicant limits the amount and	3.1.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	
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	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.	3.1.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
collection of such personal information? Where YES, describe.	Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	

1. 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	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	3.2.5 You must use or provide personal information only for the purposes to which the data subject (user) consented when it was collected or to the extent based on laws, and if you want to use or provide it otherwise, you must obtain additional consent from the data subject (user), or check if it is legal according to related laws,

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below.	and establish and implement appropriate safeguard measures.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual?	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	3.2.5 You must use or provide personal information only for the purposes to which the data subject (user) consented when it was collected or to the extent based on laws, and if you want to use or provide it otherwise, you must obtain additional consent from the data subject (user), or check if it is legal according to related laws, and establish and implement appropriate safeguard measures.

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?	of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify). Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or 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	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	3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
YES, describe.	collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Usingtheabove,theAccountabilityAgentmustverify	allowing the third party to access the personal information.
11. Do you transfer personal information to personal information processors? If YES, describe.		3.3.2 If personal information processing is outsourced to a third party, you must inform the data subject (user) of related information, e.g. the details of outsourced tasks and the third party, and obtain consent if necessary.
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 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	thattheApplicant'sdisclosuresortransfersofallpersonalinformationislimitedtothepurpose(s)ofcollection,orcompatibleorrelatedpurposes.	3.3.2 If personal information processing is outsourced to a third party, you must inform the data subject (user) of related information, e.g. the details of outsourced tasks and the third party, and obtain consent if necessary.
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? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by 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. Where the Applicant answers YES to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection	3.2.5 You must use or provide personal information only for the purposes to which the data subject (user) consented when it was collected or to the extent based on laws, and if you want to use or provide it otherwise, you must obtain additional consent from the data subject (user), or check if it is legal according to related laws, and establish and implement appropriate safeguard measures.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
13.c) Compelled by applicable laws?	• Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers YES to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers YES to 13.c, the Accountability Agent must require the Applicant to	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers NO to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	

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: • Online at point of collection • Via e-mail • Via preference/profile page	3.1.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided.

Question (*to be answered by the Applicant Organization*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	• Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated Where the Applicant answers NO, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the	3.1.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided. 3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers.	and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.

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. Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of	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:	3.1.1 Personal information should be collected legally and legitimately on a minimal scale for the provision of services, and when collecting personal information other than essential information, it should be classified as

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
their personal information? Where YES describe such mechanisms below.	• Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to	optional items and should not refuse to provide the service because the relevant information is not provided. 3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	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 their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives. 3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing

Question (*to be answered by the Applicant Organization*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Program Requirement of KISA
	their personal information, must be clear and conspicuous in order to comply with this principle.	the third party to access the personal information. 3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers NO, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	3.1.2 You must collect personal information legally with the consent of the data subject (user) or according to related laws, and if you are collecting the personal information of children under the age of 14, you must obtain the consent of their legal representatives. 3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing the third party to access the personal information. 3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
		information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.
20. What mechanisms are in place so that choices, where appropriate, can be honored in	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject (user) can access, correct or delete personal

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject (user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject (user) and defamation, is not distributed.

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. 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	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	necessary for the purpose of use. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an	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	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
attachment if necessary.	correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for 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	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	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
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	providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for	purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	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? 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 other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers.	3.2.2 You must provide the management procedure to the data subject(user) so that the accuracy, completeness and up-to-dateness of collected personal information are guaranteed to the extent necessary for the processing purpose.

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 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. 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.	1.2.4 You must select safeguard measures appropriate for the organization to handle the risks identified according to the result of risk assessment, establish the implementation plan, including priorities and schedules of safeguard measures, persons in charge and budgets, and have it approved by the management.
		1.3.1 You must effectively implement the selected safeguard measures according to the implementation plan, and the management boards must check the accuracy and effectiveness of the implementation results.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (eg password protections) • Encryption • Boundary protection (eg firewalls, intrusion detection) • Audit logging • Monitoring (eg external and internal audits, vulnerability scans) • Other (specify) The Applicant must implement reasonable	1.2.4 You must select safeguard measures appropriate for the organization to handle the risks identified according to the result of risk assessment, establish the implementation plan, including priorities and schedules of safeguard measures, persons in charge and budgets, and have it approved by the management. 1.3.1 You must effectively implement the selected safeguard measures according to the implementation plan, and the management boards must check the accuracy and effectiveness of the implementation results.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access,	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle	
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood	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	1.2.3 You must collect information on threats by type through analysis of the environment in and outside of the organization, select the right risk assessment method for

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	the organization, assess the risk in all areas of the management system at least once a year, and have acceptable risks approved by the management. 1.2.4 You must select safeguard measures appropriate for the organization to handle the risks identified according to the result of risk assessment, establish the implementation plan, including priorities and schedules of safeguard measures, persons in charge and budgets, and have it approved by the management.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information	2.2.3 You must receive an information protection pledge from employees, temporary employees, and outsiders who handle or have access to the information assets so that they can recognize internal policies, related laws,

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
(e.g. through regular training and oversight).	through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	and confidentiality obligations. 2.2.4 You must establish and operate annual awareness enhancement plans and education and training plans so that employees and related outsiders can understand the management systems and policies of the organization, and secure expertise for each job.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
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:	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	1.3.1 You must effectively implement the selected safeguard measures according to the implementation plan, and the management boards must check the accuracy and effectiveness of the implementation results.
30.a) Employee training and management or other safeguards?		2.2 Personal security

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
		2.3 Outsider security
30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?		2.9 System and service operations management
		2.10 System and service security management
30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?		2.11 Incident prevention and response
30.d) Physical security?		2.4 Physical security
31. Have you implemented a policy for secure disposal of	Where the Applicant answers **YES**, the Accountability Agent must verify the	3.4.1 You must establish internal policies related to the retention period and destruction of personal information,

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
personal information?	implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	and if it is time to destroy the personal information, e.g. the personal information retention period expires and the processing purpose is accomplished, you must immediately destroy it in a way that can guarantee the safety and completeness' of destruction.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with	2.11.1 To prevent infringements and personal information leakage, and quickly and effectively respond to incidents, you must establish systems and procedures for detecting, responding to, analyzing and sharing internal and external intrusion attempts, and build a system for cooperating with related external agencies and experts.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	this principle	
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 You must effectively operate your management system following internal policies and legal requirements. It shall be inspected at least once a year by personnel with independence and expertise. 1.4.3 You must analyze the cause of the identified management system problems, and measures to prevent recurrence shall be established and implemented by the management team to check the accuracy and effectiveness of the improvement results.
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	1.4.2 You must effectively operate your management system following internal policies and legal requirements. It shall be inspected at least once a year by

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	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.	personnel with independence and expertise. 1.4.3 You must analyze the cause of the identified management system problems, and measures to prevent recurrence shall be established and implemented by the management team to check the accuracy and effectiveness of the improvement results.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer	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,	2.3.1 If you are outsourcing part of your business (personal information handling, information protection, information system operation or development, etc.) to the outside, or using external facilities or services

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers?	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.	(Internet Data Center, cloud service, application service, etc.), you must identify the status and the legal requirements and risks from external organizations and services, and establish appropriate protective measures.
		2.3.2 If you are using external services or outsourcing business to outsiders, you must identify information protection and personal information protection requirements, and specify related contents in the contract or agreement.
		2.3.3 You must manage and supervise, e.g. periodically

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		inspect or audit, whether outsiders are taking safeguard measures according to the information protection and personal information protection requirements, specified in the contract, agreement and internal policies.

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	Where the Applicant answers **YES**, the	3.5.2 You must establish and implement the method and

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a	procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written 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? Where YES, answer questions 37(a) –	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject(user) 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**
(e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable	suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is	objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.	justified.	
38. Do you permit individuals to challenge the accuracy of their information, and to have it	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
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). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you	the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the	subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the	requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
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?		

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. • Internal guidelines	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	1.1.5 You must establish and prepare data protection and personal information protection policies and implementation documents that clearly present the data protection and personal information protection policies and directions of the organization. Also, you must have the policies and implementation documents approved by

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
or policies (if applicable, describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations ____ • Compliance with self-regulatory applicant code and/or rules ____ Other (describe) ____		the management including the CEO, and deliver them to employees and related persons in a form that they can easily understand. 1.4.1 You must periodically check the legal requirements, related to information protection and personal information protection, that the organization must comply with.
40. Have you appointed an individual(s) to be responsible for your overall compliance	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is	1.1.2 The CEO must appoint executives who can allocate resources like budgets and manpower, as the

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
with the Privacy Principles?	responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	chief information security officer who supervises information protection, and a chief privacy officer who supervises information protection, and the chief privacy officer who supervises personal information protection.
41. Do you have procedures in	Where the Applicant answers **YES,** the	3.5.2 You must establish and implement the method and

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
place to receive, investigate and respond to privacy-related complaints? Please describe.	Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR	procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
	4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	3.5.2 You must establish and implement the method and procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
		infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.
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 You must establish and implement the method and procedure for exercising rights so that the data subject(user) can access, correct or delete personal information, suspend the processing thereof, raising objections, and withdraw his/her consent more easily than the collection method and procedure, and if the data subject(user) requests it, you must immediately comply with the request and record it. Also, you must establish and implement the standards for deletion requests and temporary measures, so that information, which infringes on others' rights, e.g. violation of the data subject(user) and defamation, is not distributed.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	2.2.3 You must receive an information protection pledge from employees, temporary employees, and outsiders who handle or have access to the information assets so that they can recognize internal policies, related laws, and confidentiality obligations. 2.2.4 You must establish and operate annual awareness enhancement plans and education and training plans so that employees and related outsiders can understand the management systems and policies of the organization, and secure expertise for each job.

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. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	3.2.5 You must use or provide personal information only for the purposes to which the data subject (user) consented when it was collected or to the extent based on laws, and if you want to use or provide it otherwise, you must obtain additional consent from the data subject (user), or check if it is legal according to related laws, and establish and implement appropriate safeguard measures. 3.3.1 If personal information is provided to a third party, you must do so based on legal grounds or by obtaining the consent of the data subject (user), and establish and implement safeguard measures to safely protect personal information in the process of providing it, e.g. allowing the third party to access the personal information.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	2.3.1 If you are outsourcing part of your business (personal information handling, information protection, information system operation or development, etc.) to the outside, or using external facilities or services (Internet Data Center, cloud service, application service, etc.), you must identify the status and the legal requirements and risks from external organizations and services, and establish appropriate protective measures. 2.3.2 If you are using external services or outsourcing business to outsiders, you must identify information protection and personal information protection requirements, and specify related contents in the contract

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
• Compliance with self-regulatory applicant code and/or rules _____ Other (describe) _____		or agreement. 2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking protective measures according to the information protection and personal information protection requirements, specified in the contract, agreement and internal policies.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-compliant privacy policies and practices as	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	2.3.1 If you are outsourcing part of your business (personal information handling, information protection, information system operation or development, etc.) to the outside, or using external facilities or services (Internet Data Center, cloud service, application service, etc.), you must identify the status and the legal requirements and risks from external organizations and services, and establish appropriate protective measures.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Program Requirement of KISA**
stated in your Privacy Statement?_____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement?_____ • Follow instructions provided by you relating to the manner in which your personal information must be handled?_____ • Impose restrictions on subcontracting unless with your consent? _____		2.3.2 If you are using external services or outsourcing business to outsiders, you must identify information protection and personal information protection requirements, and specify related contents in the contract or agreement. 2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking protective measures according to 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**
• Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ • Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? Other (describe) _____		
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your	The Accountability Agent must verify the existence of such self-assessments.	2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking protective measures according to 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**
instructions and/or agreements/contracts? If YES, describe below		2.3.4 When an external contract expires, the termination of the business, or the person in charge changes, you must implement protection measures such as the return of Information assets, deletion of information system access accounts, destruction of important information, and Requesting confidentiality of acquired information.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	2.3.3 You must manage and supervise, e.g. periodically inspect or audit, whether outsiders are taking protective measures according to 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**
		2.3.4 When an external contract expires, the termination of the business, or the person in charge changes, you must implement protection measures such as the return of Information assets, deletion of information system access accounts, destruction of important information, and Requesting confidentiality of acquired information.
50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy	3.3.1 Minimum personal information necessary for provision of service must be collected legally, and if personal information other than essential information is collected, it must be classified as an option, and service provision should not be refused because such information is not provided.

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

Annex C

SIGNATURE AND CONTACT INFORMATION

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

Eun-A Na March 9th, 2023

[title] **Director**

[name of organization] **Korea Internet & Security Agency**

[Address of organization] **9 Jinheung-gil, Naju-si, Jeollanam-do, Korea, 58324**

[Email address] **eana@kisa.or.kr**

[Telephone number] **+82-61-820-1810**

The first APEC recognition for an Accountability Agent is limited to one year from the date of recognition. Recognition for the same Accountability Agent will be for two years thereafter. One month prior to the end of the recognition period, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change(e.g. ownership, structure, policies).

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

Guideline for APEC CBPR certification

Enacted on December 29, 2020.

Amended on September 28, 2022.

Chapter 1 General Provisions

Article 1 (Purpose) The purpose of this guideline is to stipulate matters necessary for the Korea Internet & Security Agency to fairly conduct APEC CBPR (Asia-Pacific Economic Cooperation Cross Border Privacy Rules) certification.

Article 2 (Definitions of terms) The terms used in this guideline are defined as follows:

1. "APEC CBPR certification" refers to the official recognition that the Certification Applicant's measures and activities to protect personal information conform to the CBPR certification criteria in [Appendix 1].
2. "Certification audit" refers to confirmation of whether the activities related to personal information protection, which are established and conducted by the applicant, conform to the CBPR certification criteria in [Appendix 1] using such methods as written and on-site review, etc.
3. "Certification committee" refers to the organization installed and operated by the President of KISA to deliberate and make decisions on the results of certification audit. <Amended on September 28, 2022>
4. "Certification auditor" refers to a person recognized by KISA as having the ability to conduct a certification audit.
5. "Certification committee member" refers to a member of the certification committee (hereinafter referred to as the committee).
6. "Substitute member" refers to a certification committee member (hereinafter referred to as the committee member) appointed to fill a vacancy in case the committee has a vacancy.
7. "Applicant" refers to the organization which applied to KISA for APEC CBPR certification.
8. "Preliminary check" refers to a procedure in which the applicant self-diagnoses the matters established and operated in accordance with the certification criteria before the certification audit, and confirms

whether the records of it and related evidence are appropriate.

9. "Re-certification audit" refers to the certification audit conducted upon application for re-certification as the term of validity expired.

10. "Defect" refers to a case where the applicant fails to meet the requirements set forth in the APEC CBPR certification criteria in [Appendix 1].

Chapter 2 Composition and operation of the certification committee

Article 3 (Roles and composition of the committee) ① The president of KISA must install and operate the committee to deliberate and make decisions on the following: <Amended on September 28, 2022>

1. The results of certification audit or re-certification audit;
2. Matters concerning the cancellation of certification or processing of objections; and
3. Matters requiring deliberation and resolution by the certification committee <Amended on September 28, 2022>

② The president of KISA selects more than 10 experts who have knowledge and experience in the field of personal information protection and are qualified as certification auditors, and use them when organizing the certification committee. <Amended on September 28, 2022>

③<Deleted on September 28, 2022>

④ The committee appoints a secretary for efficient performance of the committee's work, separate from the committee members, and the team leader in charge of the APEC CBPR certification project will be the secretary.

⑤ KISA organizes a certification committee with 3 or more committee members when there is an agenda for deliberation or decision. <Newly inserted on September 28, 2022>

⑥ Certification committee members, who participated in the certification audit of matters subject to certification deliberation/decision, cannot participate in the certification deliberation/decision process. <Newly inserted on September 28, 2022>

Article 4 (Obligations of committee members) The committee members must comply with the following ethical and security obligations:

1. The committee members objectively and fairly deliberate on the results of the certification audit and

decide on whether to grant certification.

2. The committee members should faithfully perform their duties and maintain dignity.

3. The committee members should avoid any pressure, commercial, financial or otherwise, in connection with the certification deliberation.

4. The committee members must prepare the Ethics Pledge [Appendix 15] and Information Protection Pledge [Appendix 16] of committee members [Appendix 16], and submit them to KISA in regard to compliance with the above.

Article 5 (Excluding committee members and selecting substitute committee members) ① The president of KISA excludes committee members from the committee when they violate laws or this guideline. <Amended on September 28, 2022>

② If there is a vacancy in the committee for the following reasons, a substitute committee member may be appointed.

1. If it was confirmed that a committee member received bribes, solicited favors from interested parties or exerted undue influence in the course of the committee's activities, and he or she was excluded from the committee; and <Amended on September 28, 2022>

2. If a committee member resigns.

Article 6 <Deleted on September 28, 2022>

Article 7 (Holding and operating committee meetings) ① KISA holds a committee meeting if it is deemed necessary to request deliberation and decision on the results of the certification audit or to hold a committee meeting, and deliberation and decision can be made in writing or online. <Amended on September 28, 2022>

②<Deleted on September 28, 2022>

③ The committee submits to the president of KISA the results of deliberation and decision on each item in Paragraph 1 of Article 3. <Amended on September 28, 2022>

④ Other details on the operation of the committee are stipulated in the operation manual of the certification committee. <Amended on September 28, 2022>

Article 8 (Quorum for holding a committee meeting and making a decision) ① The committee must be attended by all members of the committee except for the certification committee members who participated in the certification audit of the agenda subject to certification deliberation and decision. <Amended on September 28, 2022>

② Agenda for deliberation and decision will be passed with the consent of 2/3 or more of the committee members. <Amended on September 28, 2022>

Article 9 (Exclusion, avoidance and evasion) ① Committee members are excluded from deliberation and decision of the agenda if the agenda of the committee falls under any of the following subparagraphs:

1. Matters of direct interest to committee members themselves
2. Matters related to persons who are or were relatives of the committee members themselves;
3. Matters of direct interest to committee members themselves due to special legal relationship, etc.; and
4. Matters whose audit/investigation or inspection they were involved in before becoming committee members

② If there are circumstances in which it is difficult to expect a fair deliberation and decision from the committee members, a party to the relevant agenda may apply for a challenge to the committee, and the committee will make a decision by voting. In this case, the committee members subject to the application for challenge cannot participate in the voting.

③ If committee members fall under any of the reasons for exclusion in each subparagraph of Paragraph 1, they may voluntarily avoid deliberation and decision of the relevant agenda.

Chapter 3 Applying for Certification Audit

Article 10 (Advance preparations of the applicant) ① If the applicant intends to apply for certification, the following documents must be submitted to KISA.

1. [Appendix 2] APEC CBPR certification application
2. [Appendix 3] APEC CBPR specification
3. [Appendix 1] Self-assessment of APEC CBPR certification criteria
4. Business license or identification number

② KISA may request supplementation from the applicant if the descriptions in the documents submitted by

the applicant are incomplete or if attachments are missing.

③ The applicant must supplement the application documents within 10 days from the date of receiving the supplementary request from KISA, and if supplementation is not done by the deadline, the application for certification audit is regarded as canceled.

Article 11 (Preliminary check) ① KISA can conduct a written or on-site inspection of the applicant's preparation for audit.

② If KISA cannot conduct a certification audit due to insufficient preparation of the applicant, KISA may request supplementary measures and postpone the certification audit.

Chapter 4 Certification Audit

Article 12 (Organization of the certification audit team) ① KISA must organize a certification audit team when the certification audit schedule is confirmed.

② The certification audit team is composed of people who are recognized as having the ability to conduct the APEC CBPR certification audit, and KISA establishes and operates detailed principles for the organization and operation of the audit team.

③ An auditor belonging to KISA must be selected as the audit leader.

④ When the certification audit team is organized, the following certification auditors must be excluded:

1. Auditors who are affiliated with the applicant or have been affiliated with the applicant for the past three years
2. Auditors who have performed related tasks, e.g. security consulting and outsourced work, for the applicant in the past three years
3. Auditors who have a relationship with the applicant pursuant to Paragraph 1 of Article 9

Article 13 (Roles of the certification audit team) ① The audit team leader must perform the following roles:

1. Establishment of certification audit plans, oversight of audit and report of results
2. Job assignment of certification auditors

3. Confirmation of supplementary measures for certification audit defects

4. Evaluation of certification auditors with regard to certification audit activities

5. Preparation of certification audit result reports

6. Reporting certification audit results at the committee meeting

② Audit team members must perform the following roles:

1. Establishing audit plans for assigned audit tasks and conducting an audit

2. Preparing and submitting a certification audit defect report

3. Supporting and cooperating with the audit team leader

Article 14 (Duties of the certification auditor) ① A certification auditor must perform the following duties:

1. A certification auditor conducts an objective and fair certification audit.

2. A certification auditor must perform duties diligently and maintain dignity.

3. A certification auditor must be freed from any commercial, financial or other pressures in connection with the conduct of the certification audit.

② When participating in a certification audit, the certification auditor must sign the Code of Ethics for Certification Auditor Work in [Appendix 17] and the Security Pledge of Certification Auditors in [Appendix 18].

Article 15 (Cost of certification audit) ① KISA pays consulting fees to certification auditors according to [Attached table 2] certification auditor remuneration and travel expenses payment standards.

② When a certification auditor goes on a business trip domestically or abroad, transportation, meal, and lodging expenses are paid as fixed travel expenses in accordance with [Appendix 2] the certification auditor remuneration and travel expenses payment standards, and the amount is paid according to [Appendix 1] and [Appendix 2] of the 「Travel Rules」 of KISA.

③ KISA may charge the applicant for the expenses necessary for the certification audit.

Article 16 (Certification audit) ① The certification audit combines document-based and on-site audit of applicants.

② In the document-based audit, administrative elements are audited for compliance with [Appendix 1] by reviewing the privacy policy and evidence of policy implementation.

③ In the on-site audit, technical elements are audited by interviewing the person in charge, checking related systems, and checking vulnerabilities in order to check the results of the document-based audit and whether technical and physical protection measures have been implemented.

④ KISA prepares a [Appendix 8] defect report for problems found in the certification audit, and prepares a [Appendix 9] request for supplementary measures for defects, and requests supplementary measures from the applicant.

⑤<Deleted on September 28, 2022>

Article 17 (Supplementary measures) ① The applicant must take the supplementary measures within 40 days from the date of receiving the request for supplementary measures, fill out the supplementary measures statement in [Appendix 11], and submit it to KISA along with an official document on the completion of the supplementary measures.

② If supplementary measures are not completed within 40 days, the applicant should prepare [Appendix 11] supplementary measures statement for defects for which supplementary measures are completed, and [Appendix 12] supplementary measures summary for defects for which supplementary measures are not completed, and submit an official notice of extension of the supplementary measures. In this case, the audit team leader can additionally grant a supplementary measures period of up to 60 days if it is judged that the reason for extending the supplementary measures is justifiable.

③ The audit team leader can visit the site and check the results if on-site confirmation of the details of the supplementary measures submitted by the applicant is deemed to be necessary.

④ Completion of supplementary measures in Paragraph 2 refers to the completion of the supplementary measures completion confirmation in [Appendix 13] including signatures of the applicant's privacy officer and audit team leader. <Amended on September 28, 2022>

Article 18 (Reporting results) The audit team leader must check the details of the supplementary measures for defects and prepare a certification audit result report within 120 days from the date of completion of the audit. <Amended on September 28, 2022>

Article 19 (Suspension of audit) ① Where the applicant intentionally delays or obstructs the implementation of the certification audit or where it is deemed difficult to proceed with the certification audit due to reasons attributable to the applicant;

2. When it is believed that the applicant is not ready for certification after reviewing the relevant data submitted by the applicant;

3. If supplementary measures in accordance with Article 17 are not completed after the certification audit;

4. If it is judged that the certification audit is impossible due to natural disasters or changes in the business environment, etc.

② If the certification audit is suspended, the applicant must prepare the certification audit suspension confirmation in [Appendix 10] and submit it to KISA.

③ KISA may resume or terminate the certification audit if the reasons for suspension of the certification audit in Paragraph 1 are resolved, or according to the result of processing the objection pursuant to Article 24.

Chapter 5 Issuance and Management of Certificates

Article 20 (Issuance of certificates, etc.) ① The president of KISA notifies the applicant of the result when the result of deliberation/decision by the committee is submitted, and if the applicant is judged to meet the APEC CBPR certification criteria in [Appendix 1], the APEC CBPR certificate in [Appendix 4] must be issued.

② The certificate is valid for one year according to Paragraph 1.

③ If KISA deems it necessary, e.g. the occurrence of serious personal information protection incidents for those who have obtained the certification or the filing of complaints in accordance with Paragraph 2 of Article 25, the president of KISA may request the organization that has obtained the certification to submit separate data within the scope of the certification.

Article 21 (Management and reissuance of certificates) ① KISA must manage the details of issued certificates, e.g., certification numbers, issuance dates, and validity periods.

② An organization that has obtained certification must submit an application for reissuance of the APEC CBPR certificates in [Appendix 5] to KISA in case the certificates are lost.

③ An organization that has obtained certification must submit the APEC CBPR certificate change application in [Appendix 6] to KISA if they want to request a change in certificate details, e.g., company name, name of representative, and more.

④ KISA must submit the APEC CBPR certification performance report in [Appendix 1], including the number of certification audits, complaints received, and adjustments, to the Personal Information Protection Commission at least once a year.

Chapter 6 Follow-up management of certificates

Article 22 (Re-certification audit) ① If an organization that has obtained certification wants to extend the validity of the certificate, he or she must apply for a re-certification audit three months before the validity period of the certificate expires.

② The re-certification audit is conducted in accordance with Chapter 4.

Article 23 (Cancellation of certification) ① KISA may cancel certification through deliberation and decision of the committee when it finds any of the following reasons:

1. If certification has been obtained by false or fraudulent means or the organization that has obtained certification fails to comply with it afterwards;
2. If an organization that has obtained certification falsely publicizes details of the certification; and
3. If an organization that has obtained certification does not take necessary measures to handle personal information complaints in accordance with Paragraph 4 of Article 25

② When KISA cancels certification in accordance with Paragraph 1, it must notify the organization that has obtained the certification, take back the issued certificate, and disclose the fact.

Article 24 (Objection) ① An applicant or an organization that has obtained certification may file an objection within 15 days when notified by KISA of the deliberation result regarding certification suspension or cancellation. At this time, the organization concerned must submit the objection statement in [Appendix 7] to KISA.

② KISA may request the committee to deliberate if the objection pursuant to Paragraph 1 is deemed reasonable.

③ KISA must notify the result of handling the objection to the organization that filed the objection in writing.

Article 25 (Handling complaints related to personal information, etc.) ① Anyone who finds an organization that has obtained certification does not comply with APEC CBPR certification can file a complaint with KISA.

② Upon receipt of the complaint, KISA examines whether the reported matter falls within the APEC CBPR compliance scope of the organization that has obtained the certification, and if so, may request the organization that has obtained the certification to confirm the fact and make corrections.

③ If KISA needs to provide the personal information of the person who filed the complaint to a third party while handling the complaint, it must obtain prior consent from him or her.

④ An organization that has obtained certification must take corrective action within 30 days from the date of receiving the request for corrective action, and submit an official document and corrective action details to KISA in writing.

⑤ If an organization that has obtained certification needs to have the corrective action period extended, he or she must submit an official document about the extension and a written corrective action plan to KISA within 30 days. If KISA determines that the reason for the extension is justified, it may grant an additional 30-day corrective action period.

⑥ KISA notifies the receipt of the complaint and the result of handling the complaint to the person who filed the complaint and the organization that has obtained certification in writing or electronically.

⑦ KISA regularly discloses APEC CBPR complaint handling statistics and anonymized casebooks.

Article 26 (International cooperation) KISA cooperates with foreign law enforcement agencies or APEC CBPR accountability agents in relation to APEC CBPR certification to handle civil complaints and cooperate with law enforcement.

Article 27 (Confidentiality, etc.) Persons who are or have been engaged in certification audit, e.g., KISA, committee members and certification auditors, should not divulge confidential information obtained in the course of work or use it for purposes other than work purposes without proper authority or exceeding the

permitted authority.

Chapter 7 Miscellany

Article 28 (Establishment and revision of the manual) ① KISA can prepare and implement necessary manuals for APEC CBPR certification tasks.

② The establishment/revision of each manual is approved by the head of the department in charge of APEC CBPR certification at KISA.

③ Each manual takes effect from the date of approval, and if necessary, the head of the department in charge of APEC CBPR certification can designate an effective date and enforce it. <Newly inserted on September 28, 2022>

Addendum <December 29, 2020>

This guideline is effective from the date of approval by the head of the Management Planning Division.

Addendum <September 28, 2022>

This guideline is effective from the date of approval by the head of the Management Planning Division.

[Attached table 1]

APEC CBPR Certification Criteria

APEC CBPR Requirements (50)	
Notices: 4 **[Purpose of evaluation]** To evaluate whether data subjects are notified so that they understand the applicant's privacy policy well in relation to the collection, use and provision of personal information.	
1	The privacy policy, etc., must be disclosed so that the applicant's personal information processing practices and policies can be clearly and easily understood by data subjects.
	a) The privacy policy, etc. must include the following: · The personal information items collected and how each item is collected · The purpose of collecting and using personal information · (if applicable) If personal information is provided to a third party, or its processing is outsourced, details such as the fact and purpose of processing, personal information provided, and recipients of personal information · Name and location of organization and contact information of the personal information security officer or privacy officer · Data subjects' right to access or correct personal information, and how to exercise their rights
2	At the time when personal information is collected, the fact of personal information collection must be notified in a way that the data subject can reasonably recognize it.
3	The purpose of personal information collection must be notified at the time of personal information collection.
4	At the time of personal information collection, the fact or possibility of providing personal information to a third party must be notified.
Collection Limitation: 3 **[Purpose of evaluation]** To evaluate whether only personal information necessary for the purpose of processing specified by the applicant is collected. At this time, whether the personal information is necessary for the purpose of processing personal information can be evaluated in proportion to the achievement of the purpose. Also, whether the personal information collection method is legal and fair is evaluated.	

APEC CBPR Requirements (50)	
5	When collecting personal information, if there are other cases, e.g., direct collection or outsourcee, please include them in your explanation.
6	When personal information is collected, it should be limited to personal information necessary for the purpose of collection or related to the achievement of the purpose.
7	When personal information is collected, it must be consistent with related laws and regulations related to personal information processing, and personal information must be collected in a legal and fair way.
Use of Personal Information: 6 **[Purpose of evaluation]** To evaluate whether personal information is used only for the specified purpose of collection or for achieving "other compatible or related purposes." This principle should be applied considering the characteristics of personal information, collection context, etc. Here, use includes general use, transfer, and disclosure. The criterion for judging the 'compatibility' or 'relevance' of a purpose is judged by examining whether it has been used for a purpose in addition to the original purpose. For example, a centralized DB can be created and used for effective management of employee information, or information collected for credit loans can be used for debt collection purposes.	
8	As notified in the privacy policy, personal information must be used only for the purpose for which it was collected or for other compatible or related purposes.
9	If personal information is used for a purpose other than the purpose for which it was collected, there must be a justifiable ground, such as the explicit consent of the data subject or in accordance with related laws and regulations.
10	If you are providing (disclosing) collected personal information to other personal information controllers, please describe the details. - Personal information items for each purpose of providing personal information, whether personal information is provided within the scope of achieving the original purpose of personal information collection, etc.
11	If personal information processing is outsourced to a third party, please describe the details. - Personal information items for each outsourced task, whether or not the outsourcing is within the scope of achieving the original purpose of personal information collection, etc.
12	When personal information is provided to a third party, or personal information processing is outsourced to a third party, it must be provided or outsourced to achieve the original purpose for which the personal

APEC CBPR Requirements (50)	
	information was collected or a compatible or related purpose.
13	When personal information is provided or outsourced for a purpose other than the original purpose of collection, there must be reasonable grounds such as a) explicit consent of the data subject, b) when necessary to provide services or products at the request of the data subject, and c) in accordance with related laws and regulations. - If applicable, describe in detail the above 'other purpose' and consent method, whether the provision/outsourcing of personal information is necessary for the data subject's request, etc.
Choice: 7 **[Purpose of evaluation]** To evaluate whether data subjects have the option with regard to the collection, use, and provision (disclosure) of personal information.	
14	Individuals must be able to exercise the option with regard to personal information collection.
15	Individuals must be able to exercise the option with regard to the use of personal information by the personal information controller.
16	Individuals must be able to exercise the option with regard to the personal information controller's provision (disclosure) of personal information to third parties.
17	When the option to limit the collection, use or provision of personal information is provided, the option must be clearly and conspicuously displayed.
18	When the option to restrict the collection, use or provision of personal information is provided, the option must be expressed in a language that is easily and clearly understandable.
19	When the option to restrict the collection, use or provision of personal information is provided, the option must be implemented so that the data subject can easily exercise the options.
20	Procedures for effectively and expeditiously implementing the option of data subjects must be implemented.
Integrity of Personal Information: 5 **[Purpose of evaluation]** To evaluate whether personal information controllers keep records of personal information accurate, complete, and up to date. This principle is applied only to the extent necessary for the purpose of personal information use.	

APEC CBPR Requirements (50)	
21	Measures must be taken to verify that personal information retained is accurate, complete, and up-to-date (to the extent necessary for the purpose of using personal information).
22	Procedures for modifying inaccurate, incomplete and out-of-date personal information (to the extent necessary for the purpose of using personal information) should be established.
23	If inaccurate, incomplete, and out-of-date information affects the purpose of using personal information and is modified after personal information processing is outsourced, the outsourcee must be notified of the modification of such personal information and measures must be taken.
24	If inaccurate, incomplete and out-of-date information affects the purpose of personal information use, and if personal information is modified after it is provided to a third party, the third party must be notified of the modification of such personal information.
25	When the outsourcee becomes aware of inaccurate, incomplete or out-of-date personal information, there must be a procedure for notifying it to the outsourcee.
Security Safeguards: 10 **[Purpose of evaluation]** To evaluate whether reasonable security safeguards are implemented to prevent loss of personal information, illegal access to or provision of personal information, or misuse of personal information.	
26	A privacy policy must be established.
27	Physical, technical and managerial security safeguards must be prepared to protect personal information from risks such as information loss, illegal access, destruction, use, modification, provision, and misuse of information.
28	Security safeguards should be designed in proportion to the possibility and severity of the risk of damage, the sensitivity of information, and the context of personal information processing.
29	Measures (regular training, etc.) should be prepared to raise employees' awareness of personal information protection.
30	Each of the following security safeguards must be implemented.
	a) Employee training, management, etc.
	b) Information system and management, including network and software design, as well as information

APEC CBPR Requirements (50)	
	processing, storage, transmission, and disposal.
	c) Detecting, preventing and responding to attacks, intrusions or other security failures
	d) Physical security
31	A policy for safe destruction of personal information must be established and implemented.
32	Measures must be prepared to detect, prevent, and respond to external attacks, intrusions, or other security failures.
33	Procedures should be in place to test the effectiveness of measures to detect, prevent and respond to external attacks, intrusions or other security failures.
34	Regular risk assessments must be conducted, or security risks must be evaluated through certification by specialized organizations, and appropriate measures must be taken by reflecting the evaluation results.
35	Outsourcees must be required to take the following measures to prevent loss, illegal access, destruction, use, modification, provision, and misuse of personal information. a) An information security program proportional to the service provided and the sensitivity of personal information must be implemented. b) Privacy invasion or security breach of personal information must be notified immediately. c) Measures to correct or address security failures that resulted in privacy invasion or security breaches must be taken immediately.

Access and Correction: 3

[Purpose of evaluation]

To evaluate whether data subjects' right to access and correct personal information is guaranteed. Reasonable conditions must be considered to handle requests to access personal information, and data subjects' identity verification is also required for information security. The method of accessing and correcting personal information may differ depending on the characteristics of the personal information or other interests, and in some cases, correction or deletion of personal information may be restricted.

The right to access and correct personal information may be denied ▲when the cost of complying with the request to access and correct personal information is excessive, or when these requests and the privacy risks of individuals are

APEC CBPR Requirements (50)	
not balanced (e.g., repeated and cumbersome requests), ▲to protect the trade secrets of the institution, to prevent security breaches, or in accordance with legal grounds (even in this case, measures must be taken for information other than the relevant personal information), and ▲when there is a possibility that a third party's personal information may be infringed.	
36	Measures must be taken to comply with a request to confirm whether or not personal information of the data subject is retained.
37	In response to a request to access the personal information of the data subject, measures including the following must be taken.
	a) Measures to verify the identity of the individual requesting access
	b) Measures must be taken within a reasonable timeframe to comply with the access request.
	c) Information must be provided in a generally understandable and reasonable way (in an easy-to-read format).
	d) Information must be provided in a common communication method (example: e-mail, the same language as that of the request, etc.)
	e) If a fee is charged for accessing, the basis for calculating the cost and the rationale that it is not excessive must be presented.
38	In response to the data subject’s request for personal information modification, supplementation and deletion of personal information, measures including the following must be taken.
	a) Data subjects’ rights must be indicated in a clear and conspicuous manner.
	b) Measures must be taken to comply with the data subject’s request for correction, addition or deletion of personal information.
	c) Measures must be taken within a reasonable timeframe.
	d) The data subject must be notified of the result of measures such as correction and deletion of personal information.
	e) If the data subject's request is rejected, the reason for the rejection and contact information to inquire about additional information must be provided.

APEC CBPR Requirements (50)	
Accountability: 12 **[Purpose of evaluation]** To evaluate accountability for substantive compliance with measures to implement the protection principles of CBPR described above. Measures must be taken to ensure that these principles are observed even when personal information processing is outsourced or personal information is provided to a third party.	
39	Please indicate and explain all measures you are taking to comply with the personal information protection principles of this CBPR. a. Internal guidelines or policies must be established. b. Conclusion of a contract c. Compliance with related laws and regulations d. Compliance with self-regulatory regulations or rules e. Other (describe details)
40	A privacy officer responsible for overall compliance with the personal information protection principle should be designated.
41	Procedures for receiving, investigating, and responding to complaints related to personal information protection must be established.
42	Complaints received must be dealt with within an appropriate timeframe.
43	A corrective action plan for handling complaints must be established.
44	Employee training regarding the privacy policy or procedures, including handling complaints related to personal information infringement, must be conducted.
45	Procedures must be in place to respond to judicial authorities or government agencies' requests (subpoenas, warrants, orders, etc.) to provide personal information.
46	When personal information processing is outsourced, the outsourcee must comply with this principle in the following ways: a. It must be reflected in internal guidelines or policies. b. Specified in the contract

APEC CBPR Requirements (50)	
	c. Compliance with related laws and regulations d. Compliance with self-regulatory regulations or rules e. Other (describe details)
47	To ensure that the information processing outsourcee complies with the personal information protection principle, the following must be required. a. Implementation in accordance with the applicant's (outsourcer's) privacy policy (applying CBPR protection principles) b. Policies substantially similar to the applicant's (outsourcer's) privacy policy must be prepared and implemented. c. Personal information must be processed according to the instructions of the applicant (outsourcer). d. Subcontracting without the consent of the applicant (outsourcer) must be prohibited. ☐ e. Acquisition of CBPR certification must be requested. ☐ f. If personal information is leaked, notification to the applicant (outsourcer) must be requested. ☐ g. Other (describe details)
48	The outsourcee must be required to submit a self-assessment result to confirm compliance with the applicant's (outsourcer's) requirements (contract details, agreements, etc.).
49	Regular on-site visits or monitoring should be conducted to check whether the outsourcee complies with the applicant's (outsourcer's) requirements (contract details, agreements, etc.).
50	If personal information is provided to another third party for which it is difficult or impossible to take due diligence or reasonable action to comply with this principle, the reason why such a third party is unable to comply with this CBPR Principle and other ways to implement the safeguards at a level similar to this principle must be described. When data is provided with the consent of the data subject, it is necessary to prove that the procedure for obtaining consent is valid.

[Attached table 2] <Amended on September 28, 2022>

Certification Auditor Remuneration and Travel Expenses Payment Standards

A. Auditor remuneration

1. The remuneration for certification auditors is determined as follows according to the auditor's grade with reference to the 2020 average daily wage rate of software engineers in accordance with Paragraph 4 of Article 22 of the Software Promotion Act. At this time, auditors can be paid by applying the remuneration standard of the 「information protection and personal information protection management system certification」.

Grades of certification auditors		Advisory fee per day
Auditor	More than 7 years' experience	KRW300,000
Senior auditor	More than 10 years' experience	KRW350,000
Chief auditor	More than 15 years' experience	KRW450,000

2. If the certification auditor is an employee of KISA, an accountability agent, an auditing agency, or a public official of a related ministry, no separate audit fee will be paid.

B. Travel expenses

1. If a certification auditor takes a business trip domestically or abroad, transportation, food, and lodging expenses will be paid as fixed-rate travel expenses in accordance with KISA's work guidelines.

[Appendix 1] APEC CBPR Certification Performance Report

APEC CBPR Certification Performance Report

Accountability agent approval/renewal date:

Details	Performance
Number of new certifications	
Number of cancelled certifications	
Number of maintained certifications	

APEC CBPR certification results are submitted as above.

MMDDYYYY

President of the Korea Internet & Security Agency (Signature or seal)

To Chairperson of the Personal Information Protection Commission

Attachments	1. Certification performance details

[Appendix 2] APEC CBPR certification application

APEC CBPR Application

※ Shaded fields are not filled out by the applicant, and in [ ], mark √ where applicable.

Receipt number	Date received	Processing period

Applicant	Company name		Business license number
	Name of representative		Phone
	Address		
	e-mail		

Classification	Audit type	[ ] Initial audit [ ] Re-certification audit
	※ ISMS-P acquisition Y/N [ ] - Validity period ( ), scope of certification ( )	
	Scope of certification	

We apply for APEC CBPR certification as above.

MMDDYYYY

Applicant (representative) (Signature or seal)

To President of the Korea
Internet & Security Agency

Attachments	A copy of the APEC CBPR specification

Processing procedure

Fill out the application	→	Receipt and Preliminary check	→	Certification audit	→	Certification committee deliberation	→	Certificate issuance
Applicant		Accountability agent		Accountability agent		Accountability agent		Accountability agent

[Appendix 3] APEC CBPR Specification

APEC CBPR Specification

Audit type	[ ] Initial audit [ ] Re-certification audit ※ Certification validity period (for renewal only): *June 1, 2020 ~May 31, 2021*		
Desired date for certification audit			
Contact information	Department	Name	
	Phone	e-mail	
Management system operation period	___ years ___ months (○ Month ○○○○ Year ~ ○ Month ○○○○ Year)		
1. Number of services within the scope	*Representative website of Gojoseon Co., Ltd. OO services including*		
2. Personal information within the scope	*Honggildong shopping mall member information (00 cases), internal employee information (00 cases)*		
3. Number of persons within the scope	Internal manpower	*0 persons*	
	External manpower	*0 persons*	
	Total		
4. Number of information systems within the scope	The information system includes equipment within the scope, e.g. servers (web server, DB server, etc.), network equipment (router, L4 or higher switch, etc.), security equipment (firewall, IDS, IPS, DDoS response system, web firewall, etc.).		
5. Physical location	Location of auditing		
	Number of workplaces within the scope		
6. Number of personal information outsourcees			

<table>
<tr><td>within the scope</td><td colspan="3"></td></tr>
<tr><td rowspan="5">7. Establishment and operation of the management system</td><td colspan="2">Classification</td><td>Date</td></tr>
<tr><td colspan="2">Status and flow analysis completion date</td><td></td></tr>
<tr><td colspan="2">Risk assessment completion date</td><td></td></tr>
<tr><td colspan="2">Protective measure implementation completion date</td><td></td></tr>
<tr><td colspan="2">Management system inspection completion date</td><td></td></tr>
<tr><td rowspan="3">8. Internal policy</td><td>Classification</td><td>Document name</td><td>Final update date</td></tr>
<tr><td>Policy</td><td>and 00 others</td><td></td></tr>
<tr><td>Implementation document</td><td>and 00 others</td><td></td></tr>
</table>

※ Only the main contents are listed in the table above, and the details are listed on the next page.

※ Guidelines about details and APEC CBPR operation statement are posted on the KISA website.

[Appendix 4] APEC CBPR Certificate

APEC CBPR Certificate

1. Certification Number:
2. Company Name:
3. Name of Representative:
4. Scope of Certification:
5. Expiration date:

APEC CBPR certification is granted as above.

MMDDYYYY

President of the Korea Internet & Security Agency Official seal

CERTIFICATE OF APEC CBPR

1. Certificate Number:

2. Name of Organization:

3. Name of Representative:

4. Scope of Certification:

5. Accountability Agency:

This is to certify that the above-mentioned organization is compliant to the assessment standard for APEC CBPR.

Date of Issuance :

(name)

(official seal or signature)

President

Korea Internet & Security Agency

[Appendix 5] APEC CBPR Certificate Reissuance Application

APEC CBPR Certificate Reissuance Application

Receipt number		Date received	Processing period
Applicant	Company name		Business license number
	Representative		Phone
	Address		
	e-mail		
Certification information	Certification number		
	Scope of certification		
Reason for reissuance			

I apply for reissuance of certificate as above.

MMDDYYYY

Applicant (representative) (Signature or seal)

To: President of the Korea Internet & Security Agency

[Appendix 6] APEC CBPR certificate change request

APEC CBPR Certificate Change Request

Receipt number	Date received	Processing period

Applicant	Company name		Business license number
	Name of representative		Phone
	Address		
	e-mail		
Certification information	Certification number		
	Scope of certification		
Description of change	Before	(Korean)	
		(English)	
	After	(Korean)	
		(English)	
Reason for change			

I apply for certificate change as above.

MMDDYYYY

Applicant (representative) (Signature or seal)

To: President of the Korea Internet & Security Agency

Attachment	Documents proving that the content of the certificate needs to be changed

[Appendix 7] Objection Statement

Objection Statement

Receipt number	Date received	Processing period

Applicant	Company name		Business license number
	Name of representative		Phone
	Address		
	e-mail		
Notification	Date notified		
	Notified matters		
Objection target			
Reason for objection			

I raise an objection as above.

MMDDYYYY

Applicant
(representative) (Signature or seal)

To: President of the Korea Internet & Security Agency

Attachment	Evidence to confirm the contents of the objection

[Appendix 8] Defect Report <Amended on September 28, 2022>

Defect(Unconformity) Report			
Record date	MMDDYYYY	Applicant	
Audit type	[√] Initial audit	[ ] Re-certification audit	
Scope of certification			
Defect type	[ ] Serious defect	[√] Defect	
Certification auditor	Name	Hong Gil-dong (seal)	
Related departments			

Related provisions	**Related certification criteria**
Defect	◇ ~ is inadequate.
Operation status	o The applicant is performing ~~~ activities according to this certification criteria.
Details of defect	o Certification audit of the applicant shows that ~ is not done. (Diagrams, figures, etc. are included to make it easier for the applicant to understand)
List of evidence	o **Specification of relevant APEC CBPR certification criteria** ★APEC CBPR certification criteria★ (*In a table if necessary)* 1. Do you provide a notice (privacy policy, privacy statement) .. (omitted) .. about personal information notice about (privacy policy, privacy statement)? o **Specification of the applicant's policy/guidelines** ★Company A's privacy policy★ (*In a table if necessary)* Article 10 (Logon Management) .. (omitted) .. must be limited for management purposes, etc. **o The title of the document confirming the evidence, and name of the on-site confirmation system**

[Appendix 9] Request for Supplementary Measures <Amended on September 28, 2022>

Request for Supplementary Measures

Details of certification audit Application	Applicant	
	Audit type	[√] Initial audit [ ] Re-certification audit
	Scope of certification	
	certification criteria	☐ Attached table 1 KISA「APEC CBPR Certification Work Guideline」

☐ Details of the defect

※ The defect report for each case is attached separately.

Serious defects

Defects

Total

As above, I am notifying you of the request for supplementary measures for the certification audit defect. Please complete the supplementary measures within 40 days (by MMDDYYYY).

* It will be counted from the day after the audit end date. If the 40th day falls on a holiday, it will be counted until the day after the end of the holiday.

MMDDYYYY

KISA Audit Team Leader (seal)

1. If the completion of supplementary measures is insufficient, the audit team leader may request the applicant to take measures again, and the applicant must submit a supplementary measures statement reflecting the request for taking measures again.
2. If it is not possible to complete the supplementary measures by the deadline, a supplementary measures extension notice must be submitted along with a summary of the supplementary measures and the supplementary measures statement, and an extension of up to 60 days can be requested.

※ The performance check for the results of the supplementary measures must be completed, and signed by the audit team leader within the supplementary measures extension period. If it is not completed, the corresponding certification audit will be automatically canceled.

3. This certification audit was conducted by the sampling auditing technique, and there may be undiscovered defects.
4. The contents of this report are treated confidentially and will not be disclosed without prior consent of the applicant. However, exceptions are made when there is a court request or it is stipulated by law.

[Appendix 10] Certification Audit Suspension Confirmation <Amended on September 28, 2022>

Certification Audit Suspension Confirmation

Details of certification audit application	Applicant	
	Audit type	[√] Initial audit [ ] Re-certification audit
	Scope of certification	
	certification criteria	☐ Attached table 1 KISA「APEC CBPR Certification Work Guideline」

☐ Reasons why the certification audit is suspended

Due to the above reasons, the certification audit is suspended. Please re-apply for certification audit after supplementing the reasons for the suspension of the audit.

MMDDYYYY

KISA Audit Team Leader (seal)

I have confirmed the above and will re-apply for certification audit after preparations for the certification audit are complete.

MMDDYYYY

Privacy officer (seal)

1. The applicant is responsible for all expenses incurred before the audit was suspended, including the advisory fees of auditors.
2. If the audit is suspended due to a change in the scope of certification, the initial audit will be conducted upon re-application.
3. If you do not reapply for audit within the validity period of the certification, the certification may be canceled according to related laws and regulations.
4. The contents of this report are treated confidentially and will not be disclosed without prior consent of the applicant. However, exceptions are made when there is a court request or it is stipulated by law.

[Appendix 11] Supplementary Measures Statement

Supplementary Measures Statement

Applicant	
Audit type	[√] Initial audit [ ] Re-certification audit
Scope of certification	
Defect type	[ ] Serious defect [√] Defect
Related document	

Related provisions	**Related certification criteria**
Defect	◇ ~ is inadequate.
Details of the defect	o Certification audit of the applicant shows that ~ is not done. ※ *Copy or summarize the contents of the defect report.*
Details of supplementation and measures to prevent recurrence	☐ ※ *Details of supplementation must be described, and if necessary, it is possible to attach evidence (execution screens, documents, photographs, etc.), and create multiple pages.* ※ *If there are too many pages, they can be attached separately.* ※ *Measures to prevent recurrence must be included.*
Related documents or systems	※ *Related documents or systems if any*

Submission of the results of supplementary measures	Created by		Confirmed by		Date created	MMDDYYYY
Checking results of supplementary measures	Confirmed by (audit team leader)		Result	☐ Complete ☐ Incomplete	Date confirmed	MMDDYYYY

[Appendix 12] Supplementary Measures Summary

Supplementary Measures Summary

Details of certification audit application	Applicant	
	Audit type	[√] Initial audit [ ]re-certification audit
	Scope of certification	

- Details of supplementary measures -

(1) Details of completion

- Supplementary measures are completed for O out of O defects.

(2) Details of incompletion

- Supplementary measures are not completed for O out of O defects.

Standard item	Details of incompletion	Expected completion date
1. Privacy policy	o Disclosure of the privacy policy *(example)* - Updating the personal information collection method: completed - Checking the status of protecting data subjects' rights: in progress (~April 20, 2019) - Establishing countermeasures through derived results: scheduled (~May 10, 2019)	May 10, 2019
30. Implementation of protective measures	o Reviewing each stakeholder *(example)* - Information System Team: completed - Infrastructure Protection Team: to be reviewed on April 1, 2019 - Facility Management Team: to be reviewed on April 5, 2019	April 10, 2019
41. Handling personal information complaints	o Establishing the regulation and procedure for handing complaints *(example)* - Disclosing the contact information of the complaint handling center: complete - A solution to limit access to information on complaints: to be reviewed on April 15, 2019	April 20, 2019

※ The table above shows the progress of **those control items for which supplementary measures are incomplete** and the specific schedules.

[Appendix 13] Supplementary Measures Completion Confirmation

Supplementary Measures Completion Confirmation

Details of the certification audit application	Applicant	
	Audit type	[√] Initial audit [ ] Re-certification audit
	Scope of certification	

☐ Details of the defects

※ A separate statement of supplementary measures for each case is attached.

Details of the defects

Supplementary measures

I submit the details of the supplementary measures for APEC CBPR certification audit defects.

MMDDYYYY

Privacy officer (seal)

I confirmed that supplementary measures were completed for APEC CBPR certification audit defects.

MMDDYYYY

KISA Audit Team Leader (seal)

1. This certification audit is conducted using the sampling auditing technique, and there may be undiscovered defects.
2. The contents of this report are treated confidentially and will not be disclosed without prior consent of the applicant. However, exceptions are made when there is a court request or it is stipulated by law.

[Appendix 14] <Deleted on September 28, 2022>

[Appendix 15] Ethics Pledge of Certification Committee Members <Amended on September 28, 2022>

Ethics Pledge of Certification Committee Members

☐ Target activities: APEC CBPR certification committee activities

☐ Appointment period: MMDDYYYY - MMDDYYYY

As APEC CBPR certification committee members, we will practice the following to realize a clean and transparent society.

1. We believe that thorough compliance with laws and principles is the right way to prevent corruption, and we will conduct our work accurately and fairly in accordance with the procedures set forth in related laws and regulations.

1. We will not be tolerant of even the slightest corruption, and we will not seek the benefit of ourselves and others by relying on dishonest methods and corrupt means.

1. We will judge and act based on rationality and fairness rather than kinship, regionalism, and school connections.

1. We will not request or receive any money, goods, gifts, entertainment or service that may be related to corruption, and in case of violation, we will be held strictly responsible in accordance with related laws and regulations.

1. We will not commit 'information corruption' that causes public harm or promotes the interests of ourselves and others by illegally leaking, concealing, distorting, or manipulating various kinds of information acquired in the course of our work.

MMDDYYYY

Name (Signature)

[Appendix 16] Information Protection Pledge of Certification Committee Members

Security Pledge of Certification Committee Members

☐ Appointment period: MMDDYYYY - MMDDYYYY

As a member of KISA's APEC CBPR certification committee during the above period, I pledge to faithfully abide by related laws and regulations, and not to leak or disclose any confidential information obtained in the course of certification. I confirm that I may be punished in accordance with related laws and regulations, such as civil and criminal laws.

Affiliation :

Name : (Signature)

※ Related laws: Article 49 (Protection of Secrets) of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Article 27 (Obligation of Confidentiality) and Article 29 (Penalty Provisions) of the Act on the Protection of Information and Communications Infrastructure, Subparagraph 5 of Paragraph 1 of Article 4 (Disclosure of State Secrets, Etc.) of the National Security Act, etc.

[Appendix 17] Code of Ethics for Certification Auditor Work

Code of Ethics for Certification Auditor Work

☐ **Target: (applicant) (initial/re-certification) audit**

☐ **Period: MMDDYYYY ~ MMDDYYYY**

In carrying out the certification audit of the Korea Internet & Security Agency (KISA), we will practice the following to realize a clean and transparent society.

Ⅰ. We believe that thorough compliance with laws and principles is the right way to prevent corruption, and we will conduct our work accurately and fairly in accordance with the procedures set forth in related laws and regulations.

Ⅰ. We will not be tolerant of even the slightest corruption, and we will not seek the benefit of ourselves and others by relying on dishonest methods and corrupt means.

Ⅰ. We will judge and act based on rationality and fairness rather than kinship, regionalism, and school connections.

Ⅰ. We will not request or receive any money, goods, gifts, entertainment or service that may be related to corruption, and in case of violation, we will be held strictly responsible in accordance with related laws and regulations.

Ⅰ. We will not commit 'information corruption' that causes public harm or promotes the interests of ourselves and others by illegally leaking, concealing, distorting, or manipulating various kinds of information acquired in the course of our work.

Ⅰ. We will actively collect inconveniences, complaints, and opinions for improvement related to the performance of our work. To this end, we are operating a hotline with an official related to this work, and we will thoroughly protect the personal information of those who contact the official.

MMDDYYYY

	(seal)		(seal)
	(seal)		(seal)
	(seal)		(seal)

Audit Team Leader and (number of auditors)

[Appendix 18] Security Pledge of Certification Auditors

Security Pledge of Certification Auditors

Audit type	[√] Initial audit [ ]re-certification audit
Name of organization	
Audit period	MMDDYYYY ~ MMDDYYYY
Secure USB number	20137Xc_____ (last four digits)

I will faithfully comply with related laws and regulations in performing the APEC CBPR certification work performed by the Korea Internet & Security Agency (KISA) for the above applicants.

In addition, I pledge not to use, leak, or disclose the facts obtained in the course of certification work and the submissions of applicants for purposes other than the performance of certification work, and I confirm that violations of the above may be punished according to related laws and regulations such as civil and criminal laws.

Affiliation :

Name : **(Signature)**

MMDDYYYY

If the secure USB used during the audit period is lost, I shall be held responsible for the loss and pledge to compensate in kind.

Name: (Signature)

※ Related laws: Article 49 (Protection of Secrets) of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Article 27 (Obligation of Confidentiality) and Article 29 (Penalty Provisions) of the Act on the Protection of Information and Communications Infrastructure, Subparagraph 5 of Paragraph 1 of Article 4 (Disclosure of State Secrets, Etc.) of the National Security Act, etc.