Appendix B: PRP Framework Requirements

SECURITY SAFEGUARDS

Please note the additional column to the far right for mapping of Schellman's Certification Requirements to these APEC CBPR Framework Requirements. The yellow highlight serves to provide easy reference to the mapped areas.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	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.	*Security Safeguards* 1. Implement an information security policy that covers personal information processed on behalf of a controller.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	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 (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans) • Other (specify) The Applicant must periodically review and reassess these 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	*Security Safeguards* 2. Implement physical, technical and administrative safeguards that may include the following and periodically review and reassess the implemented measures to evaluate their relevance and effectiveness: • Authentication and access control (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans)

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
3. Describe how your organization makes 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 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.	*Security Safeguards* 3. Implement regular training and oversight of employees to ensure they are aware of the importance of, and obligations for, respecting and maintaining the security of personal information. Procedures may include the following: • Documented training program for employees • Regular staff meetings or other documented communications • Security policy signed by employees
4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	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 related to personal information. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such measures is required for compliance with this principle.	*Security Safeguards* 4. Implement measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. The measures implemented should be tested on a periodic basis and measures should be adjusted to reflect the results of the tests.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.	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.	*Security Safeguards* 4. Implement measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. The measures implemented should be tested on a periodic basis and measures should be adjusted to reflect the results of the tests.
6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?	The Accountability Agent must verify that the Applicant has in place appropriate processes to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.	*Security Safeguards* 5. Implement a notification process to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.
7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	*Security Safeguards* 6. Implement procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
8. Does your organization use third-party certifications or other risk assessments? Please describe.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	*Security Safeguards* 7. Perform periodic third-party certifications or other risk assessments and adjust the security safeguards to reflect the results of these certifications or risk assessments.

ACCOUNTABILITY MEASURES

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
9. Does your organization limit its processing of personal information to the purposes specified by the controller?	The Accountability Agent must verify that the Applicant has policies in place to limit its processing to the purposes specified by the controller.	*Accountability Measures* 1. Implement policies to ensure that processing of personal information is limited to the purposes specified by the controller.
10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?	The Accountability Agent must verify that the Applicant has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	*Accountability Measures* 2. Implement procedures to delete, update, and correct information upon request from the controller where necessary and appropriate.
11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.	The Accountability Agent must verify that the Applicant indicates the measures it takes to ensure compliance with the controller's instructions.	*Accountability Measures* 3. Implement measures to ensure compliance with the controller's instructions related to the activities of personal information processing.
12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with the PRP. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with the PRP.	*Accountability Measures* 4. Appoint an individual(s) to be responsible for the overall compliance with the requirements of the PRP.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	*Accountability Measures* 5. Implement procedures to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller.
14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders 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 notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders 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.	*Accountability Measures* 6. Implement procedures to notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information. 9.. Regularly train employees on the organization's privacy policies and procedures and related client instructions.
15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?	The Accountability Agent must verify that the Applicant has in place a procedure to notify controllers that the Applicant is engaging subprocessors.	*Accountability Measures* 7. Notify the controller of your engagement of subprocessors.
16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of each type of mechanism described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such mechanisms is required for compliance with this principle.	*Accountability Measures* 8. Implement mechanisms with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP.

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
17. Do the mechanisms referred to above generally require that subprocessors: a) Follow-instructions provided by your organization relating to the manner in which personal information must be handled? b) Impose restrictions on further subprocessing c) Have their PRP recognized by an APEC Accountability Agent in their jurisdiction? d) Provide your organization with selfassessments or other evidence of compliance with your instructions and/or agreements/contracts? If **YES**, describe. e) Allow your organization to carry out regular spot checking or other monitoring activities? If **YES**, describe. f) Other (describe)	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	*Accountability Measures* 8. Implement mechanisms with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP. Mechanisms should require subprocessors to perform the following: • Follow-instructions provided by your organization relating to the manner in which personal information must be handled • Impose restrictions on further subprocessing • Have their PRP recognized by an APEC Accountability Agent in their jurisdiction • Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts • Allow your organization to carry out regular spot checking or other monitoring activities

Question (to be answered by the Applicant Organization)	Assessment Criteria (to be verified by the Accountability Agent)	Relevant Program Requirement
18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place for training employees relating to personal information management and the controller's instructions. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this requirement.	*Accountability Measures* 9. Regularly train employees on the organization's privacy policies and procedures and related client instructions.

•

Appendix C: PRP System Intake Questionnaire

1) Name of the Organization that is seeking certification:
   _____

2) List of subsidiaries and/or affiliates to be covered by this recognition, their location, and the relationship of each to you:
   _____

Name of subsidiary and/or affiliate	Location of subsidiary and/or affiliate	Relationship of affiliate and/or subsidiary to you

3) Organization's Contact Point for PRP
   Name: _____
   Title: _____
   Email: _____
   Phone: _____

4) For what offering(s) or type(s) of processing service(s) are you applying for recognition?
   _____

SECURITY SAFEGUARDS (QUESTIONS 1-8)

The questions in this section are directed towards ensuring that when individuals entrust their information to an organization, their information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification or disclosure of information or other misuses.

1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?

   _____ Y _____ N

2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.

3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.

4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?

   _____ Y _____ N

5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.

   _____ Y _____ N

6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?

_____ Y _____ N

7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?

_____ Y _____ N

8. Does your organization use third-party certifications or other risk assessments? Please describe.

_____ Y _____ N

ACCOUNTABILITY (QUESTIONS 9-18)

The questions in this section are directed towards ensuring that you are accountable for complying with measures that give effect to the Principles stated above. Additionally, when transferring information, you 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.

9. Does your organization limit its processing of personal information to the purposes specified by the controller?

_____ Y _____ N

10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?

_____ Y _____ N

11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.

_____ Y _____ N

12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?

_____ Y _____ N

13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?

_____ Y _____ N

14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?

_____ Y _____ N

15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?

_____ Y _____ N

16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.

_____ Y _____ N

17. Do the mechanisms referred to above generally require that subprocessors:

- Follow-instructions provided by your organization relating to the manner in which personal information must be handled?_____
- Impose restrictions on further subprocessing? _____
- Have their PRP recognized by an APEC Accountability Agent in their jurisdiction? _____
- Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If **YES**, describe. _____
- Allow your organization to carry out regular spot checking or other monitoring activities? If **YES**, describe. _____
- Other (describe) _____

18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.

_____ Y _____ N

Appendix D: Complaint Statistics Template

Complaint Numbers

The total number of complaints will be reported. Where no complaints are received, the complaint statistics template will indicate “none” to ensure it is clear that no complaints were received that year. The number of complaints will be listed by year so that its clear regarding the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers to understand the reported figures and to aid in comparability there will be a note that the number reflects and actual and confirmed complaint rather than an inquiry.

Complaint Processing and Outcomes

A description of the process will be outlined.

A listing of the number of the outcomes of each complaint by the following types will be included:

- Complaints received that were outside of the scope of the program requirements or were not covered by the PRP program
- Complaints that were forwarded to the Participant
- Complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority
- Complaints received that were incomplete or the complainant was unresponsive to additional information requirements

Complaints Type

This section will include informative breakdowns of the complaints by type to provide a statistical picture of who is complaining and why.

The complaint types will be listed in the following categories:

- Complaint subject matter broken down by APEC information privacy principle (security safeguards and accountability);
- Information about complainants, when known, including the economy from which complaints have been made and industry;
- Information about the type of respondents to complaints, including industry classification (e.g. financial service activities, insurance) and size of company (e.g., small, mid-market, or large).

While some complaints will raise several different issues, the report will provide the basis upon which Schellman is reporting, for example, the principal aspect of the complaint.

Complaints Process Quality Measures

This section will outline how well the complaints resolution system is working. The timeliness of the processing will be reported, including the number or complaints that took longer than the target date to resolve.

General

Schellman will provide a comment on the various figures reported at the end of the reporting period as compared to previous periods to set the statistics in context.