Appendix B: Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

TSP Section 100
Principles and Criteria

Security Principle and Criteria Table
The system is protected against unauthorized access (both physical and logical)

<table>
<thead>
<tr>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Policies: The entity defines and documents its policies for the security of its system.</td>
</tr>
<tr>
<td>1.1 The entity’s security policies are established and periodically reviewed and approved by a designated individual or group.</td>
</tr>
<tr>
<td>1.2 The entity’s security policies include, but may not be limited to, the following matters:</td>
</tr>
<tr>
<td>a. Identifying and documenting the security requirements of authorized users</td>
</tr>
<tr>
<td>b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements</td>
</tr>
<tr>
<td>c. Assessing risks on a periodic basis</td>
</tr>
<tr>
<td>d. Preventing unauthorized access</td>
</tr>
<tr>
<td>e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access</td>
</tr>
<tr>
<td>f. Assigning responsibility and accountability for system security</td>
</tr>
<tr>
<td>g. Assigning responsibility and accountability for system changes and maintenance</td>
</tr>
<tr>
<td>h. Testing, evaluating, and authorizing system components before implementation</td>
</tr>
<tr>
<td>i. Addressing how complaints and requests relating to security issues are resolved</td>
</tr>
<tr>
<td>j. Identifying and mitigating security breaches and other incidents</td>
</tr>
<tr>
<td>k. Providing for training and other resources to support its system security policies</td>
</tr>
<tr>
<td>l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies</td>
</tr>
<tr>
<td>m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements</td>
</tr>
<tr>
<td>n. Providing for sharing information with third parties</td>
</tr>
<tr>
<td>1.3 Responsibility and accountability for developing and maintaining the entity’s system security policies, and changes and updates to those policies, are assigned.</td>
</tr>
</tbody>
</table>
## Criteria

<table>
<thead>
<tr>
<th>2.0</th>
<th>Communications: The entity communicates its defined system security policies to responsible parties and authorized users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.</td>
</tr>
<tr>
<td>2.2</td>
<td>The security obligations of users and the entity’s security commitments to users are communicated to authorized users.</td>
</tr>
<tr>
<td>2.3</td>
<td>Responsibility and accountability for the entity’s system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.</td>
</tr>
<tr>
<td>2.4</td>
<td>The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.</td>
</tr>
<tr>
<td>2.5</td>
<td>Changes that may affect system security are communicated to management and users who will be affected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.0</th>
<th>Procedures: The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.</td>
</tr>
<tr>
<td>3.2</td>
<td>Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:</td>
</tr>
<tr>
<td></td>
<td>a. Logical access security measures to restrict access to information resources not deemed to be public.</td>
</tr>
<tr>
<td></td>
<td>b. Identification and authentication of users.</td>
</tr>
<tr>
<td></td>
<td>c. Registration and authorization of new users.</td>
</tr>
<tr>
<td></td>
<td>d. The process to make changes and updates to user profiles.</td>
</tr>
<tr>
<td></td>
<td>e. Distribution of output restricted to authorized users.</td>
</tr>
<tr>
<td></td>
<td>f. Restriction of access to offline storage, backup data, systems, and media.</td>
</tr>
<tr>
<td></td>
<td>g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).</td>
</tr>
<tr>
<td>3.3</td>
<td>Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.</td>
</tr>
<tr>
<td>3.4</td>
<td>Procedures exist to protect against unauthorized access to system resources.</td>
</tr>
<tr>
<td>3.5</td>
<td>Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.</td>
</tr>
<tr>
<td>3.6</td>
<td>Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.</td>
</tr>
</tbody>
</table>
### Criteria

**Criteria related to execution and incident management used to achieve objectives**

3.7 Procedures exist to identify, report, and act upon system security breaches and other incidents.

**Criteria related to the system components used to achieve the objectives**

3.8 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

3.9 Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.10 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.

3.11 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.

**Change Management-related criteria applicable to the system’s security**

3.12 Procedures exist to maintain system components, including configurations consistent with the defined system security policies.

3.13 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.14 Procedures exist to provide that emergency changes are documented and authorized timely.

### 4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>The entity’s system security is periodically reviewed and compared with the defined system security policies.</td>
</tr>
<tr>
<td>4.2</td>
<td>There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its defined system security policies.</td>
</tr>
<tr>
<td>4.3</td>
<td>Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.</td>
</tr>
</tbody>
</table>

### Availability Principle and Criteria Table

The system is available for operation and use as committed or agreed.

**Criteria**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Policies: The entity defines and documents its policies for the availability of its system.</td>
</tr>
<tr>
<td>1.1</td>
<td>The entity’s system availability and related security policies are established and periodically reviewed and</td>
</tr>
</tbody>
</table>
approved by a designated individual or group.

1.2 The entity’s system availability and related security policies include, but may not be limited to, the following matters:

   a. Identifying and documenting the system availability and related security requirements of authorized users.

   b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.

   c. Assessing risks on a periodic basis.

   d. Preventing unauthorized access.

   e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access.

   f. Assigning responsibility and accountability for system availability and related security.

   g. Assigning responsibility and accountability for system changes and maintenance.

   h. Testing, evaluating, and authorizing system components before implementation.

   i. Addressing how complaints and requests relating to system availability and related security issues are resolved.

   j. Identifying and mitigating system availability and related security breaches and other incidents.

   k. Providing for training and other resources to support its system availability and related security policies.

   l. Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies.

   m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.

   n. Recovering and continuing service in accordance with documented customer commitments or other agreements.

   o. Monitoring system capacity to achieve customer commitments or other agreements regarding availability.

1.3 Responsibility and accountability for developing and maintaining the entity’s system availability and related security policies, and changes and updates to those policies, are assigned.

2.0 Communications: The entity communicates the defined system availability policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.
2.2 The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity’s system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system availability and system security are communicated to management and users who will be affected.

3.0 Procedures: The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.

3.2 Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.

3.3 Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity’s defined system availability and related security policies.

3.4 Procedures exist to provide for the integrity of backup data and systems maintained to support the entity’s defined system availability and related security policies.

**Security-related criteria relevant to the system’s availability**

3.5 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

   a. Logical access security measures to restrict access to information resources not deemed to be public.

   b. Identification and authentication of users.

   c. Registration and authorization of new users.

   d. The process to make changes and updates to user profiles.

   e. Restriction of access to offline storage, backup data, systems and media.

   f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

3.6 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

3.7 Procedures exist to protect against unauthorized access to system resources.
3.8 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.

3.9 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Criteria related to execution and incident management used to achieve objectives

3.10 Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.11 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

3.12 Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.13 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.

3.14 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.

Change management-related criteria applicable to the system’s availability

3.15 Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.

3.16 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.17 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system availability policies.

4.1 The entity’s system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.

4.2 There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.

4.3 Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.

Processing Integrity Principle and Criteria Table
System processing is complete, accurate, timely, and authorized.

Criteria
1.0 Policies: The entity defines and documents its policies for the processing integrity of its system.

1.1 The entity’s processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.

1.2 The entity’s system processing integrity and related security policies include, but may not be limited to, the following matters:

a. Identifying and documenting the system processing integrity and related security requirements of authorized users

b. Classifying data based on their criticality and sensitivity; that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements

c. Assessing risks on a periodic basis

d. Preventing unauthorized access

e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access

f. Assigning responsibility and accountability for system processing integrity and related security

g. Assigning responsibility and accountability for system changes and maintenance

h. Testing, evaluating, and authorizing system components before implementation

i. Addressing how complaints and requests relating to system processing integrity and related security issues are resolved

j. Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents

k. Providing for training and other resources to support its system processing integrity and related system security policies

l. Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies

m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements

1.3 Responsibility and accountability for developing and maintaining entity’s system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.

2.0 Communications: The entity communicates its documented system processing integrity policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

If the system is an e-commerce system, additional information provided on its website includes, but may not be limited to, the following matters:
a. Descriptive information about the nature of the goods or services that will be provided, including, where appropriate,
   i. condition of goods (whether they are new, used, or reconditioned).
   ii. description of services (or service contract).
   iii. sources of information (where it was obtained and how it was compiled).

b. The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters:
   i. Time frame for completion of transactions (transaction means fulfillment of orders where goods are being sold and delivery of service where a service is being provided)
   ii. Time frame and process for informing customers of exceptions to normal processing of orders or service requests
   iii. Normal method of delivery of goods or services, including customer options, where applicable
   iv. Payment terms, including customer options, if any
   v. Electronic settlement practices and related charges to customers
   vi. How customers may cancel recurring charges, if any
   vii. Product return policies and limited liability, where applicable

c. Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its website.

d. Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer’s e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.

2.2 The processing integrity and related security obligations of users and the entity’s processing integrity and related security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity’s system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.

2.4 The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.

3.0 Procedures: The entity placed in operation procedures to achieve its documented system processing integrity objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair
processing integrity commitments and (2) assess the risks associated with the identified threats.

3.2 The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies.

If the system is an e-commerce system, the entity’s procedures include, but may not be limited to, the following matters:

a. The entity checks each request or transaction for accuracy and completeness.

b. Positive acknowledgment is received from the customer before the transaction is processed.

3.3 The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.

If the system is an e-commerce system, the entity’s procedures include, but are not necessarily limited to, the following matters:

a. The correct goods are shipped in the correct quantities in the time frame agreed upon, or services and information are provided to the customer as requested.

b. Transaction exceptions are promptly communicated to the customer.

c. Incoming messages are processed and delivered accurately and completely to the correct IP address.

d. Outgoing messages are processed and delivered accurately and completely to the service provider's (SP’s) Internet access point.

e. Messages remain intact while in transit within the confines of the SP’s network.

3.4 The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies.

If the system is an e-commerce system, the entity’s procedures include, but are not necessarily limited to, the following matters:

- The entity displays sales prices and all other costs and fees to the customer before processing the transaction.

- Transactions are billed and electronically settled as agreed.

- Billing or settlement errors are promptly corrected.

3.5 There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.

**Security-related criteria relevant to the system’s processing integrity**

3.6 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

a. Logical access security measures to access information not deemed to be public

b. Identification and authentication of authorized users
c. Registration and authorization of new users

d. The process to make changes and updates to user profiles

e. Distribution of output restricted to authorized users

f. Restriction of access to offline storage, backup data, systems, and media

g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

3.7 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.

3.8 Procedures exist to protect against unauthorized access to system resources.

3.9 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

3.10 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Criteria related to execution and incident management used to achieve objectives

3.11 Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.12 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary

3.13 Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.14 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.

3.15 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have qualifications and resources to fulfill their responsibilities.

Change management-related criteria applicable to the system’s processing integrity

3.16 Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.

3.17 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.18 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).
Availability-related criteria applicable to the system’s processing integrity

3.19 Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.

3.20 Procedures exist to provide for restoration and disaster recovery consistent with the entity’s defined processing integrity policies.

3.21 Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.

4.1 System processing integrity and security performance are periodically reviewed and compared with the defined system processing integrity and related security policies.

4.2 There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.

4.3 Environmental, regulatory, and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.

Confidentiality Principle and Criteria Table
Information designated as confidential is protected by the system as committed or agreed.

Criteria

<table>
<thead>
<tr>
<th>1.0</th>
<th>Policies: The entity defines and documents its policies related to the system protecting confidential information, as committed or agreed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>The entity’s system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.</td>
</tr>
<tr>
<td>1.2</td>
<td>The entity's policies related to the system’s protection of confidential information and security include, but are not limited to, the following matters:</td>
</tr>
<tr>
<td>a.</td>
<td>Identifying and documenting the confidentiality and related security requirements of authorized users</td>
</tr>
<tr>
<td>b.</td>
<td>Classifying data based on its criticality and sensitivity that is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements</td>
</tr>
<tr>
<td>c.</td>
<td>Assessing risk on a periodic basis</td>
</tr>
<tr>
<td>d.</td>
<td>Preventing unauthorized access</td>
</tr>
<tr>
<td>e.</td>
<td>Adding new users, modifying the access levels of existing users, and removing users who no longer need access</td>
</tr>
<tr>
<td>f.</td>
<td>Assigning responsibility and accountability for confidentiality and related security</td>
</tr>
<tr>
<td>g.</td>
<td>Assigning responsibility and accountability for system changes and maintenance</td>
</tr>
</tbody>
</table>
h. Testing, evaluating, and authorizing system components before implementation

i. Addressing how complaints and requests relating to confidentiality and related security issues are resolved

j. Handling confidentiality and related security breaches and other incidents

k. Providing for training and other resources to support its system confidentiality and related security policies

l. Providing for the handling of exceptions and situations not specifically addressed in its system confidentiality and related security policies

m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements

n. Sharing information with third parties

1.3 Responsibility and accountability for developing and maintaining the entity’s system confidentiality and related security policies, and changes and updates to those policies, are assigned.

2.0 Communications: The entity communicates its defined policies related to the system’s protection of confidential information to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2.2 The system confidentiality and related security obligations of users and the entity’s confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters:

   a. How information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, back-up, and distribution or transmission of confidential information.

   b. How access to confidential information is authorized and how such authorization is rescinded.

   c. How confidential information is used.

   d. How confidential information is shared.

   e. If information is provided to third parties, disclosures include any limitations on reliance on the third party’s confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party’s confidentiality practices and controls that meet or exceed those of the entity.

   f. Practices to comply with applicable laws and regulations addressing confidentiality.

2.3 Responsibility and accountability for the entity’s system confidentiality and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.
2.5 Changes that may affect confidentiality and system security are communicated to management and users who will be affected.

### 3.0 Procedures: The entity placed in operation procedures to achieve its documented system confidentiality objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system confidentiality commitments and (2) assess the risks associated with the identified threats.

3.2 The system procedures related to confidentiality of inputs are consistent with the documented confidentiality policies.

3.3 The system procedures related to confidentiality of data processing are consistent with the documented confidentiality policies.

3.4 The system procedures related to confidentiality of outputs are consistent with the documented confidentiality policies.

3.5 The system procedures provide that confidential information is disclosed to parties only in accordance with the entity’s defined confidentiality and related security policies.

3.6 The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity’s defined system confidentiality and related security policies and that the third party is in compliance with its policies.

3.7 In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, the entity has procedures to protect confidential information in accordance with the system confidentiality practices in place when such information was received, or obtains customer consent to follow the new confidentiality practice with respect to the customer’s confidential information.

### System security-related criteria relevant to confidentiality

3.8 Procedures exist to restrict logical access to the system and the confidential information resources maintained in the system including, but not limited to, the following matters:

   a. Logical access security measures to restrict access to information resources not deemed to be public

   b. Identification and authentication of all users.

   c. Registration and authorization of new users.

   d. The process to make changes and updates to user profiles.

   e. Procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.

   f. Procedures to limit access to confidential information to only authorized employees based upon their assigned roles and responsibilities.

   g. Distribution of output containing confidential information restricted to authorized users.

   h. Restriction of access to offline storage, backup data, systems, and media.
i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

3.9 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

3.10 Procedures exist to protect against unauthorized access to system resources.

3.11 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

3.12 Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.

Criteria related to execution and incident management used to achieve the objectives

3.13 Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.14 Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.

3.15 Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.16 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined confidentiality and related security policies.

3.17 Procedures exist to help ensure that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security have the qualifications and resources to fulfill their responsibilities.

Change management-related criteria relevant to confidentiality

3.18 Procedures exist to maintain system components, including configurations consistent with the defined system confidentiality and related security policies.

3.19 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.20 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

3.21 Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.

4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.

4.1 The entity’s system confidentiality and security performance is periodically reviewed and compared with the defined system confidentiality and related security policies.

4.2 There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its system confidentiality and related security policies.
4.3 Environmental, regulatory, and technological changes are monitored, and their impact on system confidentiality and security is assessed on a timely basis. System confidentiality policies and procedures are updated for such changes as required.

### Generally Accepted Privacy Principles and Criteria

**Management**

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Management Principle and Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Management Principle: The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</td>
</tr>
<tr>
<td>1.1</td>
<td>Policies and Communications</td>
</tr>
</tbody>
</table>

**Privacy Policies**
The entity defines and documents its privacy policies with respect to the following:

- **1.1.0** Policies and Communications
  - a. Notice (See 2.1.0)
  - b. Choice and consent (See 3.1.0)
  - c. Collection (See 4.1.0)
  - d. Use, retention, and disposal (See 5.1.0)
  - e. Access (See 6.1.0)
  - f. Disclosure to third parties (See 7.1.0)
  - g. Security for privacy (See 8.1.0)
  - h. Quality (See 9.1.0)
  - i. Monitoring and enforcement (See 10.1.0)

**Communication to Internal Personnel**
Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity’s internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.

**Responsibility and Accountability for Policies**
Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity’s privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.

**1.2 Procedures and Controls**

**Review and Approval**
Privacy policies and procedures, and changes thereto, are reviewed and approved by management.

**1.2.1 Consistency of Privacy Policies and Procedures with Laws and Regulations**
Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.

**1.2.3 Personal Information Identification and Classification**
The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity’s privacy and related security policies and procedures.

**1.2.4 Risk Assessment**
A risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks.
Consistency of Commitments With Privacy Policies and Procedures

Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.

**Infrastructure and Systems Management**

The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following:

- Infrastructure
- Systems
- Applications
- Websites
- Procedures
- Products and services
- Data bases and information repositories
- Mobile computing and other similar electronic devices

The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity’s privacy policies and procedures.

**Privacy Incident and Breach Management**

A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following:

- Procedures for the identification, management, and resolution of privacy incidents and breaches
- Defined responsibilities
- A process to identify incident severity and determine required actions and escalation procedures
- A process for complying with breach laws and regulations, including stakeholders breach notification, if required
- An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate
- A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following:
  - Incident patterns and root cause
  - Changes in the internal control environment or external requirements (regulation or legislation)
- A process for periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed

**Supporting Resources**

Resources are provided by the entity to implement and support its privacy policies.

**Qualifications of Internal Personnel**

The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.

**Privacy Awareness and Training**

A privacy awareness program about the entity’s privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.

**Changes in Regulatory and Business Requirements**

For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed:
<table>
<thead>
<tr>
<th><strong>Ref.</strong></th>
<th><strong>Management Principle and Criteria</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Legal and regulatory</td>
</tr>
<tr>
<td></td>
<td>• Contracts, including service-level agreements</td>
</tr>
<tr>
<td></td>
<td>• Industry requirements</td>
</tr>
<tr>
<td></td>
<td>• Business operations and processes</td>
</tr>
<tr>
<td></td>
<td>• People, roles, and responsibilities</td>
</tr>
<tr>
<td></td>
<td>• Technology</td>
</tr>
</tbody>
</table>

Privacy policies and procedures are updated to reflect changes in requirements.

<table>
<thead>
<tr>
<th><strong>Notice</strong></th>
<th><strong>Notice Principle and Criteria</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Notice Principle:</strong> The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</td>
</tr>
</tbody>
</table>

### 2.1 Policies and Communications
#### Privacy Policies
The entity’s privacy policies address providing notice to individuals.

#### 2.1.0 Communication to Individuals

**Notice Principle:** Notice is provided to individuals regarding the following privacy policies:

- **a.** Purpose for collecting personal information
- **b.** Choice and consent (See 3.1.1)
- **c.** Collection (See 4.1.1)
- **d.** Use, retention, and disposal (See 5.1.1)
- **e.** Access (See 6.1.1)
- **f.** Disclosure to third parties (See 7.1.1)
- **g.** Security for privacy (See 8.1.1)
- **h.** Quality (See 9.1.1)
- **i.** Monitoring and enforcement (See 10.1.1)

If personal information is collected from sources other than the individual, such sources are described in the notice.

### 2.2 Procedures and Controls
#### Provision of Notice
Notice is provided to the individual about the entity’s privacy policies and procedures (a) at or before the time personal information is collected, or as soon as practical thereafter, (b) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (c) before personal information is used for new purposes not previously identified.

#### 2.2.1 Entities and Activities Covered
An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity’s privacy notice.

#### 2.2.2 Clear and Conspicuous
The entity’s privacy notice is conspicuous and uses clear language.

### Choice and Consent

#### Ref. **Choice and Consent Principle and Criteria**
### Choice and Consent Principle and Criteria

<table>
<thead>
<tr>
<th>Ref</th>
<th>Choice and Consent Principle</th>
<th>Policies and Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.</td>
<td>Privacy Policies</td>
</tr>
</tbody>
</table>

#### 3.1 Policies and Communications

**Privacy Policies**

3.1.0 The entity’s privacy policies address the choices available to individuals and the consent to be obtained.

**Communication to Individuals**

3.1.1 Individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.

**Consequences of Denying or Withdrawing Consent**

3.1.2 When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.

#### 3.2 Procedures and Controls

**Implicit or Explicit Consent**

3.2.1 Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual’s preferences expressed in his or her consent are confirmed and implemented.

**Consent for New Purposes and Uses**

3.2.2 If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.

**Explicit Consent for Sensitive Information**

3.2.3 Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.

**Consent for Online Data Transfers To or From an Individual’s Computer or Other Similar Electronic Devices**

3.2.4 Consent is obtained before personal information is transferred to or from an individual’s computer or other similar device.
Collection Principle and Criteria

4.0 Collection Principle: The entity collects personal information only for the purposes identified in the notice.

4.1 Policies and Communications

Privacy Policies

4.1.0 The entity’s privacy policies address the collection of personal information.

Communication to Individuals

4.1.1 Individuals are informed that personal information is collected only for the purposes identified in the notice.

Types of Personal Information Collected and Methods of Collection
The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.

4.2 Procedures and Controls

Collection Limited to Identified Purpose

4.2.1 The collection of personal information is limited to that necessary for the purposes identified in the notice.

Collection by Fair and Lawful Means

4.2.2 Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.

Collection From Third Parties

4.2.3 Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.

Information Developed About Individuals

4.2.4 Individuals are informed if the entity develops or acquires additional information about them for its use.

Use, Retention, and Disposal

Use, Retention, and Disposal Principle and Criteria

5.0 Use, Retention, and Disposal Principle: The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

5.1 Policies and Communications

Privacy Policies

5.1.0 The entity’s privacy policies address the use, retention, and disposal of personal information.
Communication to Individuals

5.1.1 Individuals are informed that personal information is (a) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (b) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (c) disposed of in a manner that prevents loss, theft, misuse, or unauthorized access.

5.2 Procedures and Controls

Use of Personal Information

5.2.1 Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.

Retention of Personal Information

5.2.2 Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.

Disposal, Destruction and Redaction of Personal Information

5.2.3 Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.

Access Principle: The entity provides individuals with access to their personal information for review and update.

6.0 Access Principle and Criteria

6.1 Policies and Communications

Privacy Policies

6.1.0 The entity’s privacy policies address providing individuals with access to their personal information.

Communication to Individuals

6.1.1 Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.

6.2 Procedures and Controls

Access by Individuals to Their Personal Information

6.2.1 Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.

Confirmation of an Individual’s Identity

6.2.2 The identity of individuals who request access to their personal information is authenticated before they are given access to that information.
Understandable Personal Information, Time Frame, and Cost

6.2.3 Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.

Denial of Access

6.2.4 Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity’s legal right to deny such access, if applicable, and the individual’s right, if any, to challenge such denial, as specifically permitted or required by law or regulation.

Updating or Correcting Personal Information

6.2.5 Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual’s personal information.

Statement of Disagreement

6.2.6 Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.

Disclosure to Third Parties

Ref. Disclosure to Third Parties Principle and Criteria

| 7.0    | Disclosure to Third Parties Principle: The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual. |

Policies and Communications

7.1 Policies and Communications

7.1.0 Privacy Policies

The entity’s privacy policies address the disclosure of personal information to third parties.

7.1.1 Communication to Individuals

Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires
7.1.2 Communication to Third Parties

Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.

7.2 Procedures and Controls

7.2.1 Disclosure of Personal Information

Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.

7.2.2 Protection of Personal Information

Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity’s privacy policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.

7.2.3 New Purposes and Uses

Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.

7.2.4 Misuse of Personal Information by a Third Party

The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.

Security for Privacy

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Security for Privacy Principle and Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0</td>
<td>Security for Privacy Principle: The entity protects personal information</td>
</tr>
</tbody>
</table>
8.1 Policies and Communications

Privacy Policies

8.1.0 The entity’s privacy policies (including any relevant security policies), address the security of personal information.

Communication to Individuals
Individuals are informed that precautions are taken to protect personal information.

8.1.1

8.2 Procedures and Controls

Information Security Program

8.2.1 A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas\(^1\) insofar as they relate to the security of personal information:

\(a\). Risk assessment and treatment [1.2.4]
\(b\). Security policy [8.1.0]
\(c\). Organization of information security [sections 1, 7, and 10]
\(d\). Asset management [section 1]
\(e\). Human resources security [section 1]
\(f\). Physical and environmental security [8.2.3 and 8.2.4]
\(g\). Communications and operations management [sections 1, 7, and 10]
\(h\). Access control [sections 1, 8.2, and 10]
\(i\). Information systems acquisition, development, and maintenance [1.2.6]
\(j\). Information security incident management [1.2.7]
\(k\). Business continuity management [section 8.2]
\(l\). Compliance [sections 1 and 10]

Logical Access Controls

8.2.2 Logical access to personal information is restricted by procedures that address the following matters:

---

\(^1\) These areas are drawn from ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management. Permission is granted by the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). Copies of ISO/IEC 27002 can be purchased from ANSI in the United States at [http://webstore.ansi.org/](http://webstore.ansi.org/) and in Canada from the Standards Council of Canada at [www.standardsstore.ca/eSpecs/index.jsp](http://www.standardsstore.ca/eSpecs/index.jsp). It is not necessary to meet all of the criteria of ISO/IEC 27002:2005 to satisfy *Generally Accepted Privacy Principles*’ criterion 8.2.1. The references associated with each area indicate the most relevant *Generally Accepted Privacy Principles*’ criteria for this purpose.
Ref. | Security for Privacy Principle and Criteria
--- | ---
a. Authorizing and registering internal personnel and individuals
b. Identifying and authenticating internal personnel and individuals
c. Making changes and updating access profiles
d. Granting privileges and permissions for access to IT infrastructure components and personal information
e. Preventing individuals from accessing anything other than their own personal or sensitive information
f. Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities
g. Distributing output only to authorized internal personnel
h. Restricting logical access to offline storage, backup data, systems, and media
i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)
j. Preventing the introduction of viruses, malicious code, and unauthorized software

Physical Access Controls

8.2.3 Physical access is restricted to personal information in any form (including the components of the entity’s system(s) that contain or protect personal information).

Environmental Safeguards

8.2.4 Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.

Transmitted Personal Information

8.2.5 Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other nonsecure networks, and wireless networks is protected by deploying industry standard encryption technology for transferring and receiving personal information.

Personal Information on Portable Media

8.2.6 Personal information stored on portable media or devices is protected from unauthorized access.

Testing Security Safeguards

8.2.7 Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.

Quality

Ref. | Quality Principle and Criteria
--- | ---
9.0 | Quality Principle: The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
9.1 Policies and Communications

Privacy Policies

9.1.0 The entity’s privacy policies address the quality of personal information.

Communication to Individuals

9.1.1 Individuals are informed that they are responsible for providing the entity with accurate and complete personal information, and for contacting the entity if correction of such information is required.

9.2 Procedures and Controls

Accuracy and Completeness of Personal Information

9.2.1 Personal information is accurate and complete for the purposes for which it is to be used.

Relevance of Personal Information

9.2.2 Personal information is relevant to the purposes for which it is to be used.

Monitoring and Enforcement

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Monitoring and Enforcement Principle and Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>Monitoring and Enforcement Principle: The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.</td>
</tr>
</tbody>
</table>

10.1 Policies and Communications

Privacy Policies

10.1.0 The entity’s privacy policies address the monitoring and enforcement of privacy policies and procedures.

Communication to Individuals

10.1.1 Individuals are informed about how to contact the entity with inquiries, complaints and disputes.

10.2 Procedures and Controls

Inquiry, Complaint, and Dispute Process

A process is in place to address inquiries, complaints, and disputes.

10.2.1 Dispute Resolution and Recourse

Each complaint is addressed, and the resolution is documented and communicated to the individual.

10.2.2 Compliance Review

Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans
Instances of Noncompliance
Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.

10.2.4

Ongoing Monitoring
Ongoing procedures are performed for monitoring the effectiveness of controls over personal information, based on a risk assessment [1.2.4], and for taking timely corrective actions where necessary.

10.2.5