HPOL#04
Privacy Related Issues for Outside Entities

(Version 1.0)

Table of Contents

4.1. SCOPE AND OBJECTIVES

At a minimum, government organizations will subject outside entities / third parties such as vendors, auditors, consultants, etc., to the same access restrictions to which an internal user would be subject. Since Confidential / Internal information cannot be controlled once it is distributed outside the organization, third-party access to the same must be restricted to the information they require in completing the contracted work. Government organizations must require them to formally acknowledge their responsibility for confidentiality through a written statement.

This document addresses policies related to privacy and confidentiality of information while dealing with outside entities.

This policy applies to the employees of government organizations and any person using the information technology resources of these organizations. This includes contractors, consultants, third party associates and any temporary employees of government organizations.

4.2. POLICY STATEMENT

4.2.1. ACCESS TO / DISCLOSURE OF RESTRICTED / CONFIDENTIAL / INTERNAL INFORMATION

4.2.1.1. Access to Restricted / Confidential / Internal Information

4.2.1.1.1. Access to restricted / confidential / internal information or data of government organizations must be provided to third-parties only if they have a legitimate business need for the same and must be controlled to avoid intentional / unintentional disclosure.

4.2.1.1.2. All such requests for access to restricted / confidential / internal information coming from a third-party must be forwarded to the information owner who will decide whether the request should be granted and level of access to be granted.

4.2.1.2. Disclosure of Information System Control Specifics to Third Parties

4.2.1.2.1. Employees of government organizations must not disclose to any persons outside the organization, either the information system controls that are in use in the organization or the way in which they are implemented. Exceptions will be made only if approval from the Chief Innovation Officer (CIO) is first obtained.

4.2.1.3. Signing of Confidentiality Agreements

4.2.1.3.1. Section heads / managers responsible for contracts with third-parties must ensure that the third-parties are made to sign confidentiality and compliance agreements.

Explanatory Notes

Each third-party employee must sign the confidentiality and compliance agreements, which must be kept on file by the concerned section manager.

4.2.1.4. Signing Agreements Prepared by Third Parties

4.2.1.4.1. Employees must not sign confidentiality agreements provided by third parties without the authorization of legal counsel and designated personnel of the government organization, assigned to handle intellectual property matters.

4.2.1.5. Log of Disclosed Information

4.2.1.5.1. Disclosure of confidential / restricted / internal information of government organizations to third parties must be maintained in a log indicating the information that was provided.

Explanatory Notes

This log will be important when the time arrives to recover these materials (or obtain a letter certifying the destruction of the materials) at the end of a contract.

4.2.1.6. Third Party Internal Controls

4.2.1.6.1. Depending on the sensitivity and criticality of the services or data provided, government organizations must consider commissioning or requesting a review of the service provider's internal control structure.

Explanatory Notes

The purpose of the review is to verify that any confidential / restricted / internal information of the government organization is maintained securely.

4.2.2. DISCLOSURE OF PUBLIC INFORMATION TO THIRD PARTIES

4.2.2.1. Releasing Information Classified as Public

4.2.2.1.1. Permission to disclose any government organization information to the news media / public must be obtained from management prior to release.

Explanatory Notes

Accordingly, all information to be released to the public must be reviewed by management according to an established and documented process.

4.2.2.1.2. Only the designated "owner" of the information can release such information to the public.

Explanatory Notes

Any such release to the public must be accompanied by the name of the information owner acting as the single recognised official source and point-of-contact.

4.2.2.1.3. Government organization employees are forbidden from making any public representations about the organization, unless explicitly authorized to do so by management.

4.2.3. COLLECTION AND DISCLOSURE OF CITIZEN INFORMATION

4.2.3.1. Disclosure of Restricted / Confidential / Internal Citizen Information

4.2.3.1.1. Restricted / Confidential / Internal citizen information maintained by the government organization, whether in electronic or printed form, must not be disclosed to any third party without prior and explicit consent from the affected citizen/s or the respective information owner in consultation with legal counsel.

Explanatory Notes

The necessity for obtaining explicit citizen consent will be decided by the information owner on a case by case basis.

4.2.3.1.2. Such information may be shared *within the government organization* for the purpose of improving or furthering citizen service, and/or for internal training activities, provided there is no contractual obligation with the citizen to limit the internal sharing or use of the information. Approval from the information owner/s shall be obtained before information is shared.

Explanatory Notes

Such sharing is not considered as a disclosure to a third party. When sharing knowledge / experience that is based in whole or part upon such information, in the course of delivering services to other citizens, the name or other data *that could reveal the citizen's identity must not be associated with the information being shared.*

4.2.3.2. Surreptitious Collection of Citizen Private Data Prohibited

4.2.3.2.1. Restricted / confidential information about citizens must never be stored on the systems of government organizations without first having obtained their consent.

Explanatory Notes

By prohibiting surreptitious private data gathering, citizens have more confidence, thereby improving the public image of government organizations as well as citizen loyalty.

4.2.3.3. Permissible Information to Collect from Citizens

4.2.3.3.1. Government organizations must collect, process, store and transmit only that citizen information which is necessary for the purposes of the organization.

4.2.4. RESPONSIBILITIES OF EMPLOYEES / THIRD PARTIES

4.2.4.1. Securing Restricted / Confidential Internal Information

4.2.4.1.1. All third parties accessing government organization systems must exercise due care to protect restricted / confidential / internal information of the organization from loss and unauthorized use and manipulation.

Explanatory Notes

This will include but not be limited to taking all necessary precautions related to logical (Logical Access Control Policy) and physical security (Physical and Environmental Security Policy).

4.2.4.2. Use, Distribution, Removal and Copying Information / Products

4.2.4.2.1. Any restricted / confidential / internal information of the government organization or software and related products developed by third parties and/or the government organization, must not be copied, distributed, removed or otherwise used by third parties without documented authorization from the appropriate manager of the government organization.

4.2.4.3. Conditions for Acceptance of Information from Third Parties

4.2.4.3.1. If an agent, employee, consultant, or contractor is to receive restricted / confidential information from a third party on behalf of the government organization, this disclosure must be preceded by the third party's approval of a release form / declaration from the third party’s Legal counsel.

4.2.4.4. Notification Responsibilities

4.2.4.4.1. Third parties employees are responsible for immediately informing the manager responsible for the contract, of any security breaches, including but not limited to unauthorized access to or compromise of data.

4.2.4.4.2. Any government organization employee who is aware of security violations by third parties must report them to the designated information owner.

4.2.5. Service Level Agreements

4.2.5.1. Description of Services

4.2.5.1.1. All third party service level agreements must have a detailed description of services provided by the service provider.

Explanatory Notes

Examples of description of services include but are not limited to system availability, maintenance / support services, system backups and recovery services, problem management and escalation, change management, security management and monitoring services.

4.2.5.2. System Availability

4.2.5.2.1. The Service Level Agreement must specify the different levels of system availability.

<u>Explanatory Notes</u>

Examples of the different levels of system availability are standard, critical and mission critical. The levels of system availability provide the time of the day and duration when the system should be available and operational. The Service Level Agreement must also specify the availability exclusions, e.g., scheduled maintenance, emergency maintenance, break/fix, etc.

The levels of system availability should be decided on the basis of criticality of information systems for the government organization.

4.2.5.3. Maintenance and/or Support Services

4.2.5.3.1. A detailed schedule of maintenance and/or support services for systems must be provided in the Service Level Agreement.

<u>Explanatory Notes</u>

The schedule of maintenance should include but not be limited to stating the hardware, software, technology, time period and exclusions / exceptions.

4.2.5.3.2. The Service Level Agreement must define criteria for 'emergency' situations relevant to the systems or infrastructure covered by the Service Level Agreement.

4.2.5.3.3. All Service Level Agreements must have an exclusive approach to maintenance and support in case of an emergency.

4.2.5.4. Systems Backup and Recovery

4.2.5.4.1. All Service Level Agreements must specify the procedure for systems backup and recovery.

<u>Explanatory Notes</u>

The procedure for systems backup and recovery must include but not be limited to the backup schedule, type of *backups, onsite and off-site storage locations, retention period, recovery circumstances and responsibilities of personnel accountable for this job.*

4.2.5.4.2. All changes to any backup and recovery procedure referred to in the Service Level Agreement must be authorized by the management of both government organization and service provider.

4.2.5.5. Problem Management and Escalation

4.2.5.5.1. The Service Level Agreement must contain the definition of different levels of problem severity.

Explanatory Notes

The impact of the different levels of problem severity on the government organization operations, and organization risks associated with them should be specified.

4.2.5.5.2. The Service Level Agreement must specify the elapsed time to escalate and begin trouble shooting, based on the problem severity levels.

4.2.5.5.3. A list of personnel associated with the specific information system(s) and their contact details must be provided in the Service Level Agreement.

4.2.5.6. Change Management

4.2.5.6.1. All Service Level Agreements must contain procedures and guidelines for change management compliant with the government organization's "Acquisition, Development and Maintenance of Software" Policy and associated procedures.

4.2.5.7. Security Management

4.2.5.7.1. All Service Level Agreements must specify the accountability and responsibility of personnel.

Explanatory Notes

The accountability and responsibility of personnel would need to include but not be limited to security controls for the services offered, equipment, backup devices, storage media and access to systems.

4.2.5.7.2. All Service Level Agreements must have incident management procedures and plans, for the necessary actions to be taken in the event of security breaches.

4.2.5.8. Monitoring Services

4.2.5.8.1. All Service Level Agreements must specify the schedule of reporting the status of various services offered by the service provider.

4.2.6. OUTSOURCING

4.2.6.1. Authorization for Outsourcing

4.2.6.1.1. Outsourcing of information or data processing functions or services to third party organizations must be formally authorized by the management of the government organization.

Explanatory Notes

The government organization recognizes that under certain circumstances it may be necessary to outsource some information or data processing functions or services to third party organizations. However, from an information security perspective, such outsourcing could constitute a risk to the government organization's Information assets and needs to be appropriately controlled.

4.2.6.2. Identification of Risks Associated with Outsourcing

4.2.6.2.1. Prior to outsourcing information or data processing functions or services to third parties, it is the government organization's policy that a risk assessment be conducted to identify potential risks to the government organization's Information Security.

Explanatory Notes

This risk assessment should consider the following criteria:

- *The type of information or data processing functions or services to be outsourced;*
- *The risk classification of the information or data processed by this system;*
- *The reasons for outsourcing the function or service;*
- *Background information about the third party; and*
- *The availability and effectiveness of the controls that need to be implemented to regulate and monitor the confidentiality, integrity and availability of the information processed and accessible by the third party.*

4.2.6.3. Security Requirements in Outsourcing Contracts

4.2.6.3.1. Outsourcing should be based on a contractual agreement between the government organization and the third party.

Explanatory Notes

The government organization may outsource certain information or data processing functions or services to third parties.

4.2.6.3.2. Outsourcing contracts must be consistent in all respects with the government organization's Information Security policies, procedures, standards, and guidelines.

Explanatory Notes

Outsourcing contracts must include the following conditions as a minimum:

- *The level of physical and logical security that will be provided (by the third party) to maintain the confidentiality and integrity of the government organization's information / data processed.*
- *The service level to be provided and the level of availability in the event of a disaster.*

- *Provision for confidentiality, non-disclosure and acceptable use relating to the information / data processed by the outsourced function or service.*

4.2.6.3.3. The government organization must have the right to review and audit, compliance with the terms of the outsourcing contract.

4.2.7. EXIT POLICIES

4.2.7.1. Withdrawal of Access Rights on Involuntary Termination of an Employee, Contractor or Third Party Service Provider

4.2.7.1.1. Withdrawal of access rights on involuntary termination of an employee, contractor or third party service provider shall be governed by the Exit of Personnel section detailed in the “Personnel Security Infrastructure” Policy.

4.2.7.2. Recovery of ICT Assets and Equipment

4.2.7.2.1. On termination of an employee, contractor or third party service provider, all information systems assets issued to the concerned person must be recovered prior to settlement of dues and departure from the government organization.

4.2.7.3. Withdrawal of Access Rights on Resignation / Voluntary Termination of Employment / Completion of Contractual Obligations or Services

4.2.7.3.1. Withdrawal of access rights on resignation / voluntary termination of employment / completion of contractual obligations or services shall be governed by the “Acquisition, Development, and Maintenance of Software” Policy.