HPOL#08
Communications and Operations Management

(Version 1.0)

Table of Contents

8.1. SCOPE AND OBJECTIVES

Communications and operations management is an important function that has a significant impact on information security. Due to the level of access to the information systems available at this level, detailed documented operating procedures, including an appropriate level of segregation of duties is required.

The purpose of this policy document is to ensure the right and secure operation of information processing facilities; to minimize risk due to system failures and to safeguard the integrity of information processing facilities and software. This policy also suggests guidelines to ensure secure network operations and exchange of information within the organization.

8.2. POLICY STATEMENT

8.2.1. OPERATIONS MANAGEMENT

8.2.1.1. Documented Operating Procedures

8.2.1.1.1. Operating procedures to enforce all components and requirements of the government organization's Information Security Policies, procedures, standards, and guidelines, shall be maintained and updated.

Explanatory Notes

The government organization's operational processes shall represent and comply with the content of the documented operating procedures.

8.2.1.2. Operational Change Control

8.2.1.2.1. All changes to the government organization's information systems environment must be documented, reviewed, authorized, and tested (using a test environment) prior to being made operational in the organization's production environment.

Explanatory Notes

For the purposes of this policy, the term "Changes to the government organization's information systems" will include but is not limited to the following categories of changes:

- *Changes to hardware and hardware configurations;*
- *Changes to operating systems and operating system configurations;*
- *Changes to application software programs and application software configurations;*
- *Changes to data and database configurations;*
- *Changes to user access configurations;*
- *Changes to network and communication device configurations; and*

- *Changes to configuration of physical access and environmental control devices.*

8.2.2. INCIDENT MANAGEMENT

8.2.2.1. Incident Response Plan Development

8.2.2.1.1. The government organization should develop, communicate and implement an Incident Response Plan for detecting and reporting incidents relating to exceptional situations in day to day administration of ICT and information security related areas.

8.2.2.2. Incident Response

8.2.2.2.1. The government organization requires that the identification and response to various types of potential Information Security incidents must be in accordance with the organization's Incident Response Plan.

8.2.2.3. Incident Response Responsibilities

8.2.2.3.1. The Chief Innovation Officers (CIOs) will be responsible for responding to Information Security incidents in accordance with the government organization's Incident Response Plan.

8.2.2.4. Incident Reporting

8.2.2.4.1. Government organization staff, contractors, and other users of the organization's information are responsible for reporting any confirmed or suspected security problem in a timely manner to the appropriate authority.

8.2.2.5. Incident Investigation

8.2.2.5.1. All reported incidents must be logged and classified according to specific criteria relating to the criticality of the incident as specified in the government organization's Incident Response Plan document.

Explanatory Notes

Incident response procedures shall include specific procedures to discover, protect, record, collect, identify and preserve evidence related to the incident in a manner that will not render it unacceptable in a court of law.

8.2.3. SEGREGATION OF DUTIES

8.2.3.1. Segregation of Duties in Operational Procedures

8.2.3.1.1. The government organization's ICT processes shall adopt the principle of segregation of duties to the maximum extent possible.

Explanatory Notes

This would, at a minimum, include:

- *Persons involved in operational functions must not be given additional responsibilities in ICT administration processes and vice versa.*
- *Persons involved in development processes must not be given additional responsibilities in ICT administration processes and vice versa.*

8.2.3.1.2. Where segregation of duties is not possible or practical, the process must include compensating controls.

Explanatory Notes

Examples of compensating controls include but are not limited to monitoring of activities, maintenance and review of audit trails and management supervision.

8.2.4. SEPARATION OF DEVELOPMENT, TEST AND OPERATIONAL FACILITIES

8.2.4.1. Physical and Logical Separation

8.2.4.1.1. The Development, Test and Production facilities / environments must be physically and/or logically separated.

8.2.4.2. Mutually Exclusive Access

8.2.4.2.1. Access to development, test and production environments must be mutually exclusive.

8.2.4.3. Procedures for Transfer of Software between Environments

8.2.4.3.1. Transfer of software between the development, test and operational environments will be subject to procedures as laid down by the government organization.

8.2.5. SYSTEM PLANNING AND ACCEPTANCE

8.2.5.1. Systems Acquisition and Implementation Procedures

8.2.5.1.1. All new systems or system upgrades or new versions shall be planned and acquired in accordance with Systems Acquisition and Implementation Procedures.

Explanatory Notes

Systems Acquisition and Implementation Procedures shall include specific procedures to monitor and project future capacity requirements so as to ensure that adequate processing power and storage is available.

Systems Acquisition and Implementation Procedures shall include clearly defined system acceptance criteria.

8.2.6. BACKUP AND RESTORATION

8.2.6.1. Backup and Restoration Procedures

8.2.6.1.1. Backups must be in accordance with the government organization's Backup and Restoration Procedure.

Explanatory Notes

All application and operating systems software, data (including databases), application, operating systems, user configuration information and hardware configuration information (where applicable) must be backed up.

Separate systems specific backup and restoration procedures must be developed in accordance with system requirements and vendor recommendations. These procedures must be documented and implemented during (and as part of) system implementation.

The backup and restoration procedure will determine the type of backups to be performed, the periodicity or schedule of the backup, and the protection to be provided to backup media based on the criticality of the information backed up as determined by the "Asset Classification and Control" Policy and its associated procedures.

The backup and restoration procedures must include procedures to periodically perform various levels of tests to ensure that the backup operation and media are working as expected.

8.2.6.1.2. Restoration of backups will require specific and appropriate authorization and must be performed in accordance with the government organization's Backup and Restoration Procedure.

8.2.7. OPERATOR LOGS

8.2.7.1. Logging Procedures

8.2.7.1.1. The government organization must maintain logs for all changes made and all work carried out.

Explanatory Notes

Operational procedures for operator staff shall include logging of identified scheduled and unscheduled activities including but not limited to the following:

- *System errors or events and action taken.*
- *Confirmation that scheduled tasks (backups, maintenance etc.) were completed successfully, as scheduled.*

8.2.7.1.2. Logs must be subject to periodic verification.

Explanatory Notes

The objective of verification is to ensure compliance with all operating and security procedures.

8.2.8. FAULT LOGGING

8.2.8.1. Fault Reporting

8.2.8.1.1. Users must report all incidents in which the system is unable to function as required. Such incidents are referred to as 'faults'.

8.2.8.1.2. All system faults or suspected system faults must be logged, investigated, and resolved.

8.2.8.2. Review of Logs

8.2.8.2.1. Corrective measures must be reviewed by the government organization.

Explanatory Notes

The objective of the review is to ensure that security controls have not been compromised.

8.2.9. NETWORK MANAGEMENT

8.2.9.1. Network Security

8.2.9.1.1. The government organization must implement appropriate security measures and features, to protect the network and system infrastructure.

8.2.9.1.2. The government organization must establish appropriate controls within the network and connected services.

Explanatory Notes

The objective of the controls is to prevent unauthorized access that could impact critical business information assets within the network and connected services.

Controls must be implemented to protect connected systems, and to safeguard the confidentiality and integrity of critical business information assets that pass over public networks.

8.2.9.2. Access to Network Infrastructure and Utilities

8.2.9.2.1. Logical access to networking hardware and software must be limited to authorized personnel.

8.2.9.2.2. Access to programmable network devices (e.g., routers and bridges) must be restricted to authorized personnel.

Explanatory Notes

The use of network diagnostic and security tools must be limited to specifically designated staff, and in accordance with their job responsibilities.

Access to all network configuration and security-related data, such as dial-up numbers must be limited to authorized personnel.

8.2.9.3. General Network Management Controls

8.2.9.3.1. Routers and bridges must be configured to prevent the disclosure of the configuration of the internal network to external entities.

8.2.9.3.2. Unattended network connection ports (e.g., conference rooms, empty offices, etc.) must be enabled only when needed.

8.2.9.3.3. Any services that are not required must be blocked, preferably at the firewall, but at least at the end system or server.

8.2.9.3.4. Users must only be provided with direct access to the services that they have been specifically authorized to use.

8.2.9.3.5. Users must not use dial-up modems for external connectivity, while they are connected to the government organization's internal network.

8.2.10. MEDIA HANDLING AND SECURITY

8.2.10.1. Management of Removable Computer Media

8.2.10.1.1. Removable computer media must be managed and controlled in accordance with applicable government organization procedures.

8.2.10.1.2. Media must be stored in a safe and secure environment.

8.2.10.1.3. Personnel who are not employees of the government organization, or contractors, must not be able to identify critical business information assets by their labels.

8.2.10.1.4. The previous contents of any re-usable media must be completely erased.

8.2.10.2. Disposal of Media

8.2.10.2.1. Appropriate, secure, and safe disposal of critical business information assets must be in accordance with the disposal procedures of the government organization.

Explanatory Notes

The disposal procedures must cover all media including hardcopy materials, carbon paper, one-time-use printer or fax ribbons, magnetic tapes, removable disks or cassettes, etc.

8.2.10.3. Information Handling Procedures

8.2.10.3.1. Information must be stored and handled in accordance with the government organization's information handling and storage procedures.

Explanatory Notes

The information handling procedures identify controls over the storage and handling of information that will be consistent with the classification label assigned to the information, in accordance with the "Asset Classification and Control" Policy and associated procedures.

8.2.10.4. Security of System Documentation

8.2.10.4.1. System documentation must be protected from unauthorized access.

Explanatory Notes

The system or application owner must authorize or approve distribution lists for system documentation. This list must be restricted to a minimum number of parties.

Valid documentation that supports the government organization, and which is used by programming, operations, and user personnel, must be developed, maintained, and protected. Access to this documentation must be restricted to personnel performing official duties.

8.2.10.5. Offsite Storage of Backups and Documentation

8.2.10.5.1. Data and key documentation should be maintained at an offsite location. Whenever the backup media is moved to and from the offsite location it should be carried in a sealed and tamper-proof envelope or pouch. The backup media should be stored in fire-proof cabinet.

8.2.11. EXCHANGE OF INFORMATION AND SOFTWARE

8.2.11.1. Information and Software Exchange Agreements

8.2.11.1.1. Formal agreements must be established for the exchange of critical business information assets or software with outside organizations.

Explanatory Notes

These agreements must include manual and/or electronic exchanges.

These agreements must reflect the sensitivity of the critical business information assets being exchanged and must describe any protection requirements.

These agreements must, at a minimum, specify management responsibilities, notification requirements, packaging and transmission standards, courier identification, responsibilities and liabilities, data and software ownership, protection responsibilities and measures, and encryption requirements.

8.2.11.2. Security of Media in Transit

8.2.11.2.1. Appropriate measures should be adopted by the government organization to prevent the unauthorized disclosure / dissemination of critical business information assets while in transit.

Explanatory Notes

Such measures would include but not be limited to the following:

- *Physical media must be properly protected and controlled.*
- *Reliable transport or couriers must be used.*
- *Packaging must be sufficient to protect the contents from any physical damage.*

8.2.11.3. Electronic Commerce Security

8.2.11.3.1. Electronic commerce arrangements must be specifically authorized in accordance with the government organization's Electronic Commerce security procedures.

8.2.11.3.2. Electronic commerce arrangements will only be entered into with known parties on the basis of a formal written agreement.

Explanatory Notes

The agreement will include but not be limited to addressing of legal, commercial and electronic commerce security requirements and responsibilities.

8.2.11.4. Security of Publicly Available Systems

8.2.11.4.1. Information will made available on publicly available systems only in accordance with the government organization's "Privacy and Citizen Information Protection" Policy and associated procedures.

8.2.11.5. Electronic Office Systems and Other Forms of Information Exchange

8.2.11.5.1. Electronic Office Systems should be used in accordance with the government organization's "Information Systems Acceptable Use" Policy and management guidelines.

8.2.11.5.2. The government organization's resources must not be used for personal use.

Explanatory Notes

Resources include but are not restricted to e-mail, voice-mail, video conferencing, faxes, telephone, Internet services, hardware, software, printers, copiers, hardcopy, or electronic media.

Personal use includes but is not limited to personal advertisements, solicitations or promotions of any outside business, political lobbying or promoting political activities, or any commercial purpose other than official government organization business.

8.2.11.5.3. Appropriate procedures should be defined for telephone conversations.

Explanatory Notes

Procedures relating to telephone conversations should include but not be limited to the following:

- *Staff should not reveal sensitive or classified information over the telephone unless the telephone*

lines have been specifically secured for this purpose, for example, through the use of encryption.

- *Staff should not enter into conversations or reveal any information over the telephone where the identity of the caller cannot be determined.*
- *Where appropriate, staff must confirm telephone conversations by creating, signing, and acknowledging a formal written transcript of the conversation.*
- *Staff should not discuss confidential matters or reveal confidential / classified information in public places and/or outside government organization premises.*
- *Staff should not reveal or store confidential messages on answering machines or voice-mail services.*
- *All parties to a telephone call must be notified in advance if the call is to be recorded.*

8.2.11.5.4. Appropriate procedures should be defined for Fax Machines.

Explanatory Notes

Procedures relating to fax machines should include but not be limited to the following:

- *Sensitive or confidential information must only be faxed where a more secure means of communication is not available.*
- *Both the sender of the information and the intended recipient must authorize the transmission of the information before the transmission.*
- *All fax messages should include a confidentiality clause prohibiting the recipient from disclosing the information if such a fax is received in error.*
- *Any fax received in error must be destroyed and its sender notified, if this is possible.*