HPOL#11
Compliance Measurement

(Version 1.0)

Table of Contents

11.1. SCOPE AND OBJECTIVES

The government organization must comply with applicable requirements to maintain its eligibility to conduct business with certain third parties and in certain forums. The government organization must also ensure its operations uphold the laws of society from an ethical standpoint as well as to protect and maintain its good reputation.

The government organization shall assess legal and regulatory requirements applicable to the organization and will perform procedures to uphold and to monitor compliance with these requirements.

Security policies, standards, and procedures are developed and deployed to prevent and detect security incidents. Breaches of these requirements may result in serious damage or disruption to the government organization.

This Policy establishes requirements for the government organization's enterprise-wide compliance with information security policies, standards, procedures, guidelines and applicable laws and regulations.

11.2. POLICY STATEMENT

11.2.1. COMPLIANCE POLICY

11.2.1.1. Compliance with Legal Requirements

11.2.1.1.1. The design, operation management and use of the government organization's information systems and related facilities must comply with all applicable legal, regulatory or contractual security requirements.

11.2.1.1.2. The System Security Manuals for each information system must include documentation of statutory, regulatory and contractual requirements associated with the system and procedures to assure its compliance.

11.2.1.2. Intellectual Property Rights

11.2.1.2.1. The government organization will recognize and respect intellectual property rights associated with its information systems.

<u>Explanatory Notes</u>

The government organization must comply with:

- *Copyright requirements associated with proprietary material, software, and designs acquired by the government organization.*
- *Licensing requirements limiting the usage of products, software, designs and other material acquired by the government organization.*

11.2.1.2.2. The government organization must ensure continued compliance with product copyright restrictions and licensing requirements.

11.2.1.3. Data Protection and Privacy of Personal Information

11.2.1.3.1. The government organization will comply with privacy requirements imposed by statutory, regulatory, and contractual requirements.

11.2.1.3.2. The Chief Innovation Officers (CIOs) will provide guidance to government organization Sections and users on the responsibility and requirements to maintain privacy.

11.2.1.3.3. Data owners will inform the Chief Innovation Officers (CIOs) of any changes to the retention, use or disclosure of private information.

11.2.1.4. Compliance with Security Policy

11.2.1.4.1. Management and information owners of the government organization have day-to-day responsibility for ensuring compliance with security procedures.

11.2.1.4.2. All staff accept responsibility for knowledge of their security requirements, and for self-assessing their individual compliance.

11.2.1.4.3. Periodic checks and reviews will be performed to assess the government organization's compliance with security policies.

11.2.1.5. Prevention of Misuse of Information Processing Facilities

11.2.1.5.1. Authorized uses of information processing facilities will be defined and communicated to staff as the only acceptable uses of the facilities.

11.2.1.5.2. Facility use will be monitored, as approved by legal counsel, for appropriate compliance with laws and with government organization policies, procedures, standards, and guidelines.

11.2.1.6. Safeguarding of Organizational Records

11.2.1.6.1. The government organizational records relating to information security must be protected and stored in accordance with the organization's corporate policy on maintenance of such records and the requirements of applicable laws and regulations.

Explanatory Notes

Government organizational records relating to information security include but are not limited to system logs, audit logs, configuration setting records, change control logs, and user access authorization documentation, in electronic and/or hard-copy format.

11.2.1.6.2. Government organizational records should be afforded protection based on the relevance and importance of the records, and shall be stored in a manner appropriate to the media on which they are recorded.

11.2.1.7. Collection of Evidence

11.2.1.7.1. Evidence collected for the purposes of presentation in a court of law during a civil or criminal action shall be collected in conformance with the relevant rules of evidence (if any) as laid down by the law and applicable to the relevant court of law in which the evidence is to be presented.

11.2.1.8. Technical Compliance Checking

11.2.1.8.1. The government organization’s information systems implementations and associated documentation must be reviewed immediately after implementation and thereafter at predefined intervals.

Explanatory Notes

The objective of the review is to verify that the government organization’s information systems implementations and associated documentation are compliant with Security Standards and System Security Manuals developed for each individual system.

11.2.1.8.2. The compliance review must be performed by appropriately qualified personnel.

11.2.1.9. Detection of Non-compliance

11.2.1.9.1. All personnel who detect any non-compliance issue must immediately report it to designated management personnel of the government organization.

11.2.1.9.2. All personnel who detect any non-compliance issue should not contact any external authorities without prior authorization from designated management personnel of the government organization.

11.2.1.9.3. All personnel must follow a defined procedure for reporting non-compliance issues and should not investigate the issues on their own.

11.2.2. INFORMATION SYSTEMS AUDITS

11.2.2.1. Timing of Information Systems Audits

11.2.2.1.1. Audits of operational information systems shall be planned and performed at periodic intervals with the agreement of the information systems' owner.

Explanatory Notes

Where system audits require access to the system or data or includes the use of software tools and utilities, such audits should be conducted with the knowledge, cooperation and consent of the owners of the information system.

Relevant precautions should be taken to protect the information system and data from damage or disruptions as a result of the audit or audit tools.

11.2.2.2. Usage of System Audit Tools

11.2.2.2.1. The usage of system audit tools is subject to authorization, restrictions, and controls and is in accordance with specific guidelines for this purpose.

Explanatory Notes

Systems audit tools include, but is not limited to, monitoring software, data extraction and manipulation software and utilities that may or may not be an intrinsic part of an information systems software suite.

11.2.2.2.2. Appropriate controls will be implemented with the usage of system audit tools.

Explanatory Notes

The controls will at a minimum:

- *Prevent the possible misuse of system audit tools (for example, to extract confidential information without appropriate authorization).*
- *Ensure that the integrity of the information system and associated data is maintained.*
- *Avoid possible disruptions to the information systems as a result of the usage of such tools.*

11.2.2.3. Audit Trails

11.2.2.3.1. Audit trail features in the database as well as application systems should always be kept enabled.

11.2.2.3.2. Audit logs should be periodically generated using reports in application systems or by other approved means.

Explanatory Notes

Audit logs for modification of, at a minimum, master file records, parameter files, and key transaction entries, should be generated.

11.2.2.3.3. It is the responsibility of process owners to identify the required transaction level audit trails and exception reports depending upon clear business process control objectives.

11.2.2.3.4. Procedures should be implemented for the periodic review of audit logs.

Explanatory Notes

Follow-up and monitoring procedures for issues identified should also be stipulated.