HPOL#12
Information Systems Acceptable Use

(Version 1.0)

Table of Contents

12.1. SCOPE AND OBJECTIVES

The government organization considers its information resources (i.e., information maintained in electronic form and systems that process, store, or transmit such information) as assets.

This policy addresses the need of the government organization to impose certain responsibilities on the users of information resources to ensure its legality, confidentiality, integrity and availability.

Compliance with this Policy is essential in creating an environment that is conducive to sound security practices.

12.2. POLICY STATEMENT

12.2.1. ACCEPTABLE USAGE

12.2.1.1. Usage of Information Systems

12.2.1.1.1. Users are only permitted to utilize the government organization’s information resources for business purposes for which they have been authorized.

Explanatory Notes

Usage of the government organization’s information systems and resources for personal usage or on behalf of a third party (i.e., personal client, family member, political or religious or charitable or school organization, etc.) is strictly prohibited.

12.2.1.2. Introduction of Unauthorized Copies of Licensed Software and Hardware

12.2.1.2.1. Introduction of unauthorized copies of licensed software and hardware (piracy / copyright and/or patent infringement) to the government organization’s information resources and the copying of such material is prohibited.

12.2.1.2.2. The storage, processing, or transmittal of such unauthorized copies of licensed software and hardware by the government organization’s employees, contractors, or associates, is strictly prohibited.

12.2.1.3. Introduction of Freeware and Shareware Applications

12.2.1.3.1. Introduction of freeware and shareware software whether downloaded from the Internet or obtained through any other media to the government organization’s information systems will be subject to a formal evaluation and approval process.

12.2.1.3.2. Freeware and shareware applications must be evaluated and tested by the government organization before installation on the government organization’s information resources is permitted.

12.2.1.4. Introduction of Pornographic Material

12.2.1.4.1. Introduction of pornographic material into any government organization information systems environment is strictly prohibited.

12.2.1.4.2. The storage, processing, or transmittal of pornographic material on the government organization's information systems, by government organization employees, contractors, or associates, is strictly prohibited.

12.2.1.5. Usage of Information Resources to Store, Process, Download, or Transmit Data

12.2.1.5.1. Usage of the government organization information systems to store, process, download, or transmit data that can be construed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment is strictly prohibited.

12.2.1.5.2. Downloading, redistribution and printing of copyrighted articles, documents, or other copyrighted materials to government organization information systems is strictly prohibited.

12.2.1.5.3. Receiving, printing, transmitting, or otherwise disseminating confidential information in violation of government organization policy or proprietary agreements is strictly prohibited.

Explanatory Notes

Confidential information will include but not be limited to proprietary data and government organization secrets.

12.2.1.5.4. Downloading inappropriate material for personal use is strictly prohibited.

Explanatory Notes

Inappropriate material would include but not be limited to picture files, music files, and video files.

12.2.1.6. Due Diligence

12.2.1.6.1. Each user has the responsibility to immediately notify designated management personnel of the government organization of any evidence or suspicion of any security violation.

Explanatory Notes

Security violations would include but not be limited to:

- *Unauthorized access to network, telecommunications, or computer systems;*
- *The apparent presence of a virus on a personal computer;*
- *The apparent presence of any information resource prohibited by this policy;*
- *Apparent tampering with any file for which the user established restrictive discretionary access controls; and*
- *Violation of this Policy or any other Information Security policy or procedure by another user, employee, contractor or third party service provider.*

12.2.1.6.2. Each user has the responsibility to prevent unauthorized access of information resources in his/her possession or control.

Explanatory Notes

Unauthorized access would include but not be limited to viewing of information resources. Information resources in the possession or control of the user would include but not be limited to portable computers, desktop terminals / computers, printouts and floppy / tape media.

12.2.1.6.3. Each user is responsible for providing access security against relatives, friends and neighbours, customers / clients, vendors, and unknown visitors.

Explanatory Notes

In situations where such people must be provided access (e.g., a vendor who has come to install a product or make repairs), the user must oversee and monitor the actions of the individual/s given temporary access.

12.2.1.7. Games

12.2.1.7.1. Games are not permitted and must be removed from all systems.

12.2.1.8. Introduction of Destructive Programs

12.2.1.8.1. Introduction of destructive programs is strictly prohibited.

Explanatory Notes

Destructive programs would include but not be limited to viruses and self-replicating code. The intentions of destructive programs could include but not be limited to causing intentional damage, gaining unauthorized access, and inhibiting production on the government organization's information systems.

12.2.1.9. External Services

12.2.1.9.1. All users must limit their usage of external services to authorized business purposes only in accordance with this policy, standards, and procedures regarding such usage and as approved by the user's management.

Explanatory Notes

Usage of external services would include but not be limited to bulletin boards, on-line service providers, Internet sites, and commercial data bases.

12.2.1.9.2. All users must comply with the policies, standards, and procedures of the external service that they are using.

Explanatory Notes

This statement is subject to the following exceptions:

- *Where this Policy is more stringent than the external policy, standard, or procedure.*

- *Where the external policy, standard, or procedure does not cover a specific issue covered here.*

- *Where an external policy, standard, or procedure does not exist.*

12.2.1.9.3. Any exploration of the public domain with regard to research is acceptable provided the users comply with the government organization policies, standards, and procedures regarding such usage and they comply with the policies, standards, and procedures of the explored site.