Recommended by Information System Steering Committee: December 20, 2011
Recommended by President's Council: February 10, 2012
Approved by Executive Committee: March 7, 2012

NAIT *Guideline*

ITM.1.2

Acceptable Use of NAIT's Technology Resources

Implementation Date: March 7, 2012 Replaces: OA 6.31,OA6.32, OA6.33, OA6.34 and OA6.35

Table of Contents

1.0 Guideline

The Institute provides information processing facilities to NAIT users to support the teaching, learning, research; and the strategic direction and mandate of NAIT. These resources are valuable assets to be used and managed responsibly to ensure their integrity, security and availability for educational and business activities.

This guideline applies to all Institute information and computing, electronic communications, and networking resources connected to Institute facilities and the users and creators of these resources.

The Director, Department of Information Services, shall be responsible for the development, administration and maintenance of procedures to be implemented in compliance with these Guidelines.

2.0 Background

The purpose of this guideline is to outline the acceptable use of computer equipment and the Internet at NAIT. These rules are in place to protect the user and NAIT. Inappropriate use exposes NAIT to risks including virus attacks, breaches of network systems and services, and violation of legislation.

The Department of Information Services' (ISD) intention for publishing Acceptable Use Guidelines are not to impose restrictions that are contrary to NAIT's established culture of openness, trust and integrity. ISD is, however, responsible for, and committed to protecting the Institute's users, business partners and the Institute from illegal or damaging actions by individuals, either intentional or accidental.

Effective security is a team effort involving the participation and support of every Institute user who deals with information and/or information systems, and it is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

3.0 Parameters

3.1. General Use and Ownership

3.1.1. While NAIT desires to provide a reasonable level of privacy, users should be aware that the data they create on NAIT's systems remains the property of NAIT. Because of the need to protect NAIT's network, management cannot guarantee the confidentiality of non-Institute related information stored on a network device or computer belonging to NAIT. Users also need to be aware that if data is on NAIT's system, it is in the control and custody of NAIT pursuant to the Freedom of Information and Protection of Privacy Act (FOIP) and therefore may be required to be disclosed in the event of an access request for information received by NAIT pursuant to FOIP.

3.1.2. Users are responsible for exercising good judgment regarding the reasonableness of personal use, and for taking good care of equipment loaned out to them.

3.1.3. All sensitive information should be password protected. If sensitive information is sent outside of NAIT the document should be password protected before it is sent via electronic mail or otherwise electronically transmitted.

3.1.4. For security and network maintenance purposes, authorized individuals within NAIT may monitor equipment, systems and network traffic at any time.

3.1.5. NAIT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this guidance.

3.1.6. Only licensed software may be installed on NAIT's computing devices. Auditing software may be used remotely to determine which software packages are present on each computer. NAIT staff may be asked to verify licensing and if unlicensed software is found it will be removed from the computing devices immediately.

3.1.7. All access to the NAIT Network from the Internet must be through a firewall(s) that have been selected and implemented by NAIT.

3.1.8. NAIT's technology resources have been provided to you to enable you to successfully carry out NAIT's mandate. You are responsible for the appropriate use of equipment assigned to you.

3.1.9. Computer equipment, including mobile devices, supplied by NAIT must not be altered in any fashion.

4.0 Security and Information

4.1 Passwords must be secure and accounts cannot be shared. Authorized users are

responsible for the security of their passwords and accounts. System level passwords should be changed regularly.

4.2 All computing devices should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging off when the computer will be unattended.

4.3 Personal devices must be connected to NAIT's network resources by ISD. ISD can only complete the connection of personally owned devices to NAIT's network resources after the requestor has signed the appropriate agreements and/or consent forms and the required security agents have been installed on the personally owned device.

4.4 Postings by users from a NAIT email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NAIT, unless posting is in the course of business duties.

4.5 Users must use extreme caution when opening email attachments or following links received from unknown senders, as these may contain viruses, e-mail bombs, or Trojan horse code. Also, attachments or links should only be opened if the user is expecting them. Users should also be aware that email addresses can be spoofed to make them think the sender is known.

4.6 It is the responsibility of the user to properly identify, file, retain and dispose electronic information.

4.7 All collection, use and disclosure of personal information involving electronic systems will be done in accordance with the requirements of the Freedom of Information and Protection of Privacy Act (FOIPP).

4.8 All collection, transmission and storage of Cardholder Data must comply with the Payment Card Industry Data Security Standard (PCI_DSS).

5.0 Unacceptable Use

The following activities are prohibited, and under no circumstances may a user of NAIT use NAIT-enabled technology resources services to engage in any activity that is illegal under provincial, federal or international law. The list below is by no means exhaustive, but it provides a framework for activities which fall in the category of unacceptable use:

5.1. System and Network Activities

5.1.1. Violations of the rights of any individual or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by the Institute.

5.1.2. For-Profit activities not sanctioned by NAIT.

5.1.3. Gambling activities.

5.1.4. Unauthorized copying of copyrighted materials including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the NAIT or the end user does not have an active license.

5.1.5. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, email bombs, etc.).

5.1.6. Revealing account passwords to others, or allowing the use of your account by others. This includes family members when working from home.

5.1.7. Using NAIT computing assets to actively engage in procuring, transmitting, storing

or viewing pornographic material.

5.1.8. Making fraudulent offers of products, items, or services.

5.1.9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

5.1.10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, 'disruption' includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

5.1.11. Port scanning or security scanning and executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.

5.1.12. Circumventing user authentication or security of any host, network or account.

5.1.13. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).

5.1.14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

5.1.15. Disclosing any NAIT information that is not otherwise public.

5.2. Electronic Communications Activities

5.2.1. Electronic Communications includes, but is not limited to email, text messages and social media communications.

5.2.2. Sending unsolicited electronic messages, including the sending of 'junk mail' or other advertising material to individuals who did not specifically request such material (spam).

5.2.3. Any form of harassment via electronic communication, whether through language, frequency, or size of messages.

5.2.4. Unauthorized use, or forging, of email header information.

5.2.5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5.2.6. Creating or forwarding 'chain letters', or other pyramid schemes of any type.

5.2.7. Use of unsolicited communication originating from within NAIT's networks (spam) to advertise any products.

5.2.8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6.0 Enforcement

Users must be aware that their electronic communications and Internet sites accessed can be monitored without prior notice. Allegation or suspected inappropriate use of NAIT's computer equipment and internet will be investigated by authorized individuals at NAIT. Employees who are found to be in non-compliance with this Guideline will be subject to appropriate disciplinary action up to and including termination of employment.