BRITISH COLUMBIA
INSTITUTE OF TECHNOLOGY

Guideline

Information Security

Guideline No.:	3502-GU1
Policy Reference:	3502
Category:	Information Management
Department Responsible:	Information Technology Services
Current Approved Date:	2011 May 04

Purpose

This guideline applies directly to BCIT Policy 3502, Information Security. This guideline states best practices and requirements for the protection of BCIT's information assets.

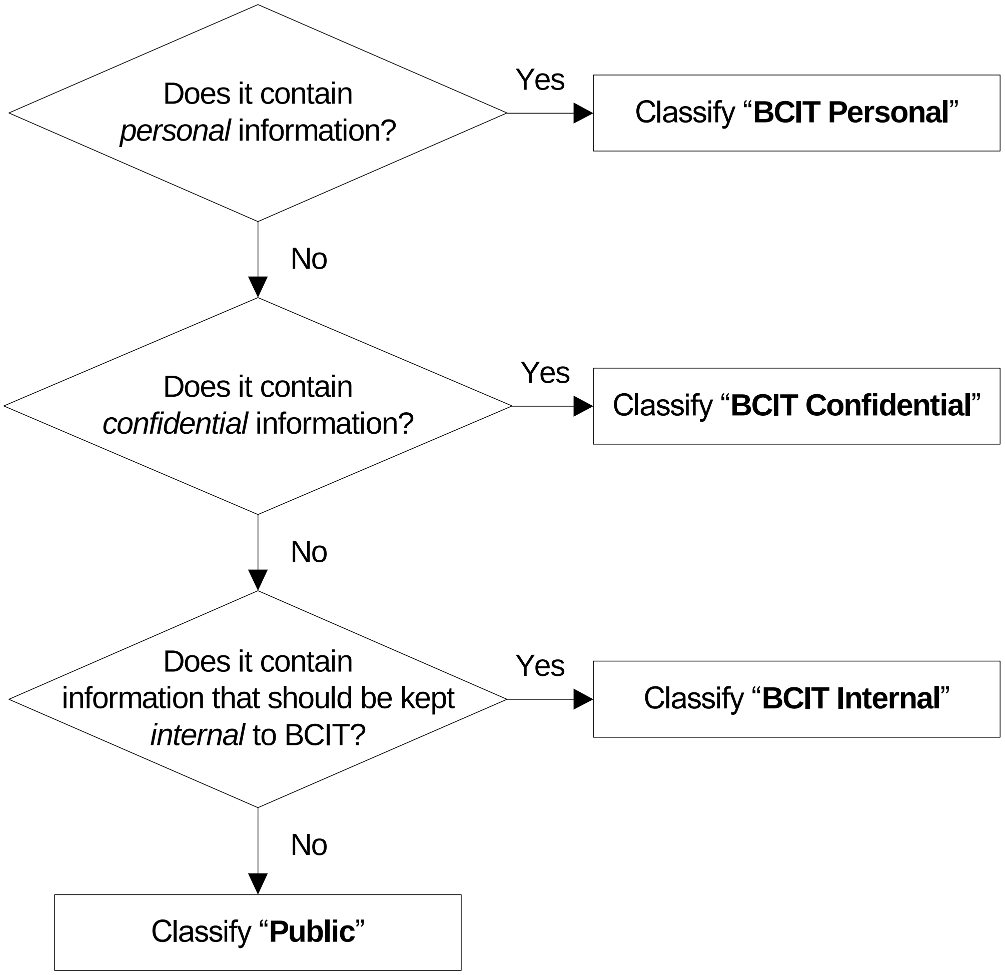
Table of Contents

Guideline

1. Classifying Information Assets

Cross-reference: Policy 3502 sections 1.1.2 (Information Owners), 2.2.2

Information owners are responsible for determining the classification of their information. The diagram below gives an overview of how to classify information.


Does it contain *personal* information?
Yes
Classify "**BCIT Personal**"
No
Does it contain *confidential* information?
Yes
Classify "**BCIT Confidential**"
No
Does it contain information that should be kept *internal* to BCIT?
Yes
Classify "**BCIT Internal**"
No
Classify "**Public**"

If information has not been classified, as an interim control, it should be considered as "*BCIT Internal*" until it is properly classified.

Some information will be classified only as "*BCIT Confidential*". If, however, information is classified as "*BCIT Personal*", it is also considered "*BCIT Confidential*" under this information classification scheme.

In addition to information security classifications BCIT users are required to assign a Directory of Records Classification to records according to BCIT policy 6701, BCIT Records Management.

Guideline

BCIT Personal

- **Description**: Information that contains personal information that if improperly disclosed could cause serious loss of privacy to an individual or to many individuals. BCIT Personal information is available to authorized users only with a business need to know. A formal Freedom of Information and Protection of Privacy (FOIPOP) request is required for non-routine disclosure (outside of BCIT) of BCIT Personal information.
- **Examples**: BCIT Personal information includes, but is not limited to:
  - Date of birth
  - Social Insurance Number
  - Drivers' license numbers
  - Home address and phone number
  - Medical information
  - Financial information
  - Passwords and passphrases
  - Educational records
  - Employment records including performance evaluations, appointment records
  - Professional opinion about employee, coworker
- **Risk Impacts**: BCIT Personal information risk impacts include, but are not limited to:
  - Loss of personal or individual privacy
  - Privacy complaints to BCIT
  - Privacy complaints at the Office of the Information and Privacy Commissioner (OIPC) of B.C.
  - Litigation

BCIT Confidential

- **Description**: Information that contains sensitive Institute information that if improperly disclosed could cause loss of: confidence in BCIT; competitive advantage; damage to partnership; relations and reputation. BCIT Confidential information is available to authorized users only with a business need to know. A formal FOIPOP request is required for non-routine disclosure (outside of BCIT) of BCIT Confidential information.
- **Examples**: BCIT Confidential information includes, but is not limited to:
  - Research data and intellectual property
  - Patent applications, trademarks and trade secrets
  - Confidentiality agreements signed by BCIT employees
  - Drafts of strategic plans, annual reports and financial statements
  - Contracts and other legal documents and material
  - Internal audit reports and working papers and files
  - Payroll information and data
  - Certain management information
  - Security response plans
  - Information about security related incidents
  - Network diagrams, IP addresses and data about sensitive network segments and systems
  - Penetration testing reports
  - Locations of hazardous material storage
- **Risk Impacts**: BCIT Confidential information risk impacts include, but are not limited to:

Guideline

  - Loss of reputation or competitive advantage
  - Loss of confidence in BCIT
  - Loss of trade secrets or intellectual property
  - Financial loss
  - High degree of risk if corrupted or modified
  - Litigation

BCIT Internal

- **Description**: Information that contains Institute data and is used in the day-to-day operations of the Institute or a department. BCIT Internal information is available to authorized users only and is not routinely disclosed. A formal FOIPOP request is required for non-routine disclosure (outside of BCIT) of BCIT Internal information.
- **Examples**: BCIT Internal information includes, but is not limited to:
  - Administration procedures
  - Draft marketing information
  - Vendor or service provider contracts
  - Internal communications regarding projects, etc.
  - Departmental policies and procedures
  - Floor plans, access codes, etc.
  - Employee lists and user id's
  - Teaching materials
  - Planning documents
  - Ordinary staff meeting agendas and minutes
- **Risk Impacts**: BCIT Internal information risk impacts include, but are not limited to:
  - Unfair competitive advantage
  - Disruption to business if not available
  - Low degree of risk if corrupted or modified
  - Loss of reputation

Public

- **Description**: Information that is available to the general public, routinely disclosed, and is created in the normal course of business that is unlikely to cause harm.
- **Examples**: Public information includes, but is not limited to:
  - Information that is approved to be publicly posted on:
    - BCIT website
    - Brochures, campus maps, etc.
    - Course descriptions
  - Published marketing information
  - Published annual reports
  - BCIT policies
  - Rates and fees
  - Contact information (general information line, program and course information line, media relations line, etc.)
  - Job postings
  - Public health information
- **Risk Impacts**: Public information risk impacts include, but are not limited to:
  - Little or no impact
  - Minimal inconvenience if not available
  - If lost, changed or denied would not result in legal effects
  - Loss of reputation

Guideline

2. Labelling Information Assets

Cross-reference: Policy 3502 section 2.2.5

Both hard copy and electronic information must be clearly labelled with its confidentiality classification so that authorized users are aware of the classification.

The actual labelling procedure will vary depending on the medium in which the information is stored. The following table identifies some common labelling methods for various types of information assets.

Type	Procedure
Hard copy documents	Rubber ink-stamps for each level may be needed to mark hardcopy documents received from outside the organization. **Marking and labels:** stamps must contain one of the following markings: • BCIT Personal • BCIT Confidential • BCIT Internal • Public
Electronic mail	Identify security classification in subject line of e-mail, if classified as personal, or confidential. **Marking and labels:** subject line of e-mail must contain one of the following markings: • **[PERS]** for BCIT Personal • **[CONF]** for BCIT Confidential
Electronic documents	Filenames must contain classification labels as specified below in Marking and labels. Identify security classification in document metadata. If the electronic document is to be printed or viewed in PDF format, the security classification should appear on every page, including the cover page (this can be done by including the classification in the header/footer or by use of a watermark). Information about the department, which created the document and date of creation, should be included. **Marking and labels:** document metadata, or visual representation of the security classification must contain one of the following markings: • BCIT Personal • BCIT Confidential • BCIT Internal • Public Filenames of electronic documents must contain with one of the following markings: • **[PERS]** for BCIT Personal • **[CONF]** for BCIT Confidential • **[BCIT]** for BCIT Internal • **[PUBLIC]** for Public

Guideline

Data, databases and business applications	Identify classification in system/application metadata. Labels may be required for online screen displays and reports generated by IT systems. **Marking and labels:** document metadata, or visual representation of the security classification must contain one of the following markings: • BCIT Personal • BCIT Confidential • BCIT Internal • Public
Other media	The security classification may be identified on adhesive labels applied to other media such as diskettes, CDs, DVDs, and videocassettes. A message with the classification label should be displayed when the information stored on the media is accessed. **Marking and labels:** visual representation of the security classification must contain one of the following markings: • BCIT Personal • BCIT Confidential • BCIT Internal • Public

3. Establishing Information Ownership

Cross-reference: Policy 3502 section 2.2.1

An information owner is the BCIT employee who decides security classification of the specified information.

The following are steps how to establish information ownership:

- A person who creates or collects information object is its owner.
- A person who extracts information object from an information source and creates another source is the information owner for the new source.
- A person who only administratively collects or extracts information objects in order to enter them into another information source is not the information owner for such information objects. In such cases, the business function manager for that information source is the information owner.

Ownership may be transferred with the agreement of both parties.

Guideline

4. Information Handling Principles

Cross-reference: Policy 3502 sections 5.7.1, 5.8.2

Media and Hard Copy Documents

	BCIT Personal / BCIT Confidential	BCIT Internal	Public
Duplication	Information Owner to determine permissions	Duplication for business purposes only	No special requirements
Mailing	• Double-sealed envelope; no classification marking on external envelope; classification marking on inside envelope (signed to reveal evidence of tampering) • Confirmation of receipt at discretion of Information Owner	Mailing requirements determined by Information Owner	No special requirements
Manual transmission	• Sealed envelope with classification marking; passed by hand between people who have the need to know • May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the need to know and there is no opportunity for any unauthorized person to view the information	Information Owner to define requirements	No special requirements
Disposal	Physical destruction beyond ability to recover (see Procedure 3502)	Controlled physical destruction (see Procedure 3502)	No special requirements
Storage	Locked up when not in use	Master copy secured against destruction	Master copy secured against destruction
Read access	Owner establishes user access rules (generally highly restricted)	Owner establishes user access rules (generally widely available)	No special requirements
Review of classification level	Information Owner to establish specific review date (not exceed one year)	Information Owner to review at least annually	No special requirements

Guideline

Electronically Stored Information

	BCIT Personal / BCIT Confidential	BCIT Internal	Public
Storage on fixed media (access controlled)	Encrypted	Unencrypted	Unencrypted
Storage on fixed media (not access controlled)	Encrypted	Unencrypted	Unencrypted
Storage on removable media	Encrypted	Unencrypted	Unencrypted
Read access to information (includes duplication)	Information Owner to authorize individual users or roles	Information Owner to define permissions on user, group, or function basis	No special requirements
Update access to information	Information Owner to authorize individual users or roles	Information Owner to define permissions on user, group, or function basis	Information Owner to define permissions
Delete access to information	Information Owner to authorize individual users or roles; user confirmation required	Information Owner to define permissions on user, group, or function basis; user confirmation required	Information Owner to define permissions
Print hard copy of information	Output to be routed to a predefined, monitored printer	Information Owner to define permissions	No special requirements
Disposal of electronic media (tapes, CD/DVD, hard disks, etc.)	Physical destruction beyond ability to recover	Physical destruction	No special requirements
Deletion of information	Delete by fully writing over information where possible	Delete information through normal platform delete command, option, or facility	No special requirements
Review of classification level	Information Owner to establish specific review date (not exceed one year)	Information Owner to review at least annually	Information Owner to review at least annually

Guideline

Electronically Transmitted Information

	BCIT Personal / BCIT Confidential	BCIT Internal	Public
By **electronic messaging** (e-mail, instant messaging)	• Encrypted • Confirmation of receipt required	Information Owner to define requirements	No special requirements
By BCIT **voice-mail**	• Confirmation of receipt required (sender) • Remove message after receipt (recipient)	Information Owner to define requirements	No special requirements
By **phone**	See Procedure 3502	Information Owner to define requirements	No special requirements
By **wireless or cellular phone**	Do not transmit	Information Owner to define requirements	No special requirements
By **LAN** (local area network)	• Encrypted • Confirmation of receipt required	Information Owner to define requirements; encryption is recommended if information is transmitted through any wireless network, and any non-BCIT wired network	No special requirements
By **WAN** (wide area network)	• Encrypted • Confirmation of receipt required	Information Owner to define requirements; encryption is recommended	No special requirements
By **FAX**	Attended at receiving FAX (see Procedure 3502)	Information Owner to define requirements	No special requirements

For routine disclosure (i.e. BCIT business processes) of BCIT Personal or BCIT Confidential information, the Information owner must review a class of recipients (i.e. individual users or roles) prior to sending the information to any of them. The review is required every time there is a change in the class of recipients.

For non-routine disclosure the sender of BCIT Personal or BCIT Confidential information must obtain permission from Information Owner every time prior to sending the information to a recipient.

Recipient must be notified by phone before the information is sent to him/her. Receipt of BCIT Personal or BCIT Confidential information must be confirmed over the phone as well.

Guideline

If encryption is used, password/passphrase to decrypt the information must not be stored or transmitted along with the encrypted information. Passwords/passphrases are considered BCIT Confidential, appropriate transmission method must be chosen.

If BCIT Personal or BCIT Confidential information is mistakenly transmitted to the wrong person, or is otherwise compromised through transmission, and you cannot get the information back, notify your supervisor and the information owner. Information owner should promptly notify the individual(s), whose personal information has been compromised, telling them the kind of information that has been compromised and steps that are being taken.

5. Minimum Logging Standards

Cross-reference: Policy 3502 section 5.6.8

Automated mechanisms must be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents.

The selection of auditable events of an information system must be based upon classification of information accessible through the system:

BCIT Personal / BCIT Confidential / BCIT Internal

1. Generate audit records for the following events:
   a) User account management activities
   b) System shutdown
   c) System reboot
   d) System errors
   e) Application shutdown
   f) Application restart
   g) Application errors
   h) File creation
   i) File deletion
   j) File modification
   k) Failed and successful log-ons
   l) Security policy modifications
   m) Use of administrator privileges
   n) File access (where additional requirements determined by System Owner / Information Owner)
2. Enable logging for any perimeter devices that control access to BCIT Personal / BCIT Confidential / BCIT Internal information for the following areas:
   a) Log packet screening denials originating from both trusted and un-trusted networks
   b) User account management
   c) Modification of packet filters
   d) Application errors
   e) System shutdown and reboot
   f) System errors
   g) Modification of proxy services.

Guideline

3. Generate transaction logs where additional requirements determined by System Owner / Information Owner.
4. Verify that proper logging is enabled in order to audit administrator and privileged accounts (e.g. database administrators, network administrators, system administrators, application administrators) activities.
5. Generate audit records for the following events in addition to those specified in other controls:
   a) All successful and unsuccessful authorization attempts every time user credentials are presented.
   b) All changes to logical access control authorities (e.g. rights, permissions).
   c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
   d) The audit trail must capture the enabling or disabling of audit report generation services.
   e) The audit trail must capture command line changes, batch file changes and queries made to the system (e.g. operating system, application, and database) under privileged accounts.
6. Send all log data specified in the previous sections 1a, 1i, 1j, 1k, 1l, 1m, 1n, 2a, 2b, 2c, 2g, 4, and 5 to the centralized logging service. Copies of log data may also be kept locally.

Public

1. Generate audit records (where additional requirements determined by System Owner / Information Owner) for the following events:
   a) User account management activities
   b) System shutdown
   c) System reboot
   d) System errors
   e) Application shutdown
   f) Application restart
   g) Application errors
   h) File creation
   i) File deletion.
2. Enable logging for any perimeter devices that control access to Public information for the following areas:
   a) Log packet screening denials originating from un-trusted networks
   b) Packet screening denials originating from trusted networks
   c) User account management
   d) Modification of packet filters
   e) Application errors
   f) System shutdown and reboot
   g) System errors.
3. Verify that proper logging is enabled in order to audit administrator and privileged accounts (e.g. database administrators, network administrators, system administrators, application administrators) activities.
4. Send all log data specified in the previous sections 1a, 2b, 2c, 2d, and 3 to the centralized logging service. Copies of log data may also be kept locally.

Guideline

6. Logs Retention

Cross-reference: Policy 3502 section 5.10.1

Audit records must be retained to provide support for after-the-fact investigations of security incidents:

- Retain audit records for a minimum of 90 days, and archive old audit records in the original log format.
- Retain audit record archives for a minimum of 1 year.

7. Extent, Frequency, and Retention of System Backups

Cross-reference: Policy 3502 section 5.5

Controls must be put in place to restore systems and data in the event of loss. System backups (onto tape or permanent media) must be in place for any business-critical application.

Backups must be made regularly - as often as daily, depending on the requirements of the business - and should be stored off-site to prevent loss or damage.

Wherever possible, backup strategy (e.g. replication) should be tested continuously as a part of ongoing system maintenance. If this is not possible then periodic test restores should be performed regularly to ensure the continued viability of the backup copies. Logs of restore tests must be kept as long as the backups are retained.

Backup data must always be created and stored in a highly secure fashion. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media (see Information Handling Principles).

System owners are responsible for establishing the extent, frequency, and retention of system backups, which must reflect the business requirements of the Institute, the security requirements of the information involved, and the criticality of the information to the continued operation of the Institute.

For each system and data type, system owners identify and document the backup schedule and type of backup used. Type of backup information in the schedule may include:

- Frequency (e.g. hourly, daily, weekly, monthly)
- Type of backup (e.g. full, incremental, or differential backup; imaging; replication)
- Type of backup media (e.g. CD, DVD, network share, backup service provided by IT Services)

Practice for extent, frequency, and retention of system backups in BCIT environment delivered as a service by IT Services is as follows:

- Backups should be run on a regular basis based on requirements.
- Backups are typically run as ongoing incremental backups. The first backup is a full

Guideline

backup followed by incrementals forever. Databases for Banner are typically archived.

- Backups should include all user level information at a minimum.
- Currently, all default backups retain 7 generations of a file and the database archives are retained for 17 days.
- All backup data is copied to physical tape and sent offsite twice weekly.

8. Protection Against Malicious Code

Cross-reference: Policy 3502 sections 5.4.2, 5.4.3

To protect against malicious code you must use anti-malware solutions and you must comply with the following best practices:

DO

… scan all media for malicious code before they are used.
… save email attachments, including compressed files (e.g. zip files), to local drive or media and scan before they are opened.
… scan all email-attached files with your anti-virus software even from people you know if the anti-virus software is not configured to do an on-demand scanning.
… restrict the use of administrator-level privileges.
… ensure that systems are up-to-date with operating system and application upgrades and patches (e.g. automatic Windows update, anti-virus update, Adobe Reader update, web browser update, etc.)
… report every virus that is not automatically cleaned by the virus protection software to IT Services Helpdesk.

DO NOT

… disable or bypass virus protection software.
… alter the settings for the virus protection software in a manner that will reduce the effectiveness of the software.
… alter the automatic update frequency of the virus protection software and operating system updates to reduce the frequency of updates.
… open suspicious emails or email attachments from unknown senders, or suspicious or unexpected attachments from known senders.
… send or receive executable files (e.g. EXE files, COM files, SCR files, BAT and CMD files, CPL files, VBS and VBE files) via email, instant messaging, or peer-to-peer file sharing services. Be aware that recipients' email systems may remove them. These types of files are often used by viruses to infect your system.
… download or execute any types of files from un-trusted sources.
… click on suspicious web browser popup windows.
… visit web sites that may contain malicious content (e.g. sites flagged as dangerous by your browser, warez sites, porn sites, etc.)

Guideline

9. Additional Access Protection Conditions and Requirements

Cross-reference: Policy 3502 section 6.2.4

Some systems may require additional protection mechanisms based on time of day, location, and additional authentication requirements. If so, consideration should be given but not limited to:

- User identity (e.g. two-factor authentication for all users with privileged user rights, and/or access to BCIT Personal and BCIT Confidential information)
- Time of day (e.g. no access after business hours if the user is allowed to log in during business hours only)
- Location (e.g. no access from outside of BCIT network if the user is allowed to log in from BCIT network only)
- Network Access Control / Network Access Protection (e.g. workstations that lack antivirus, patches, or host intrusion prevention software are not allowed to access the BCIT network)

10. Access Controls in BCIT Network

Cross-reference: Policy 3502 section 5.6.5

The following recommendations are meant as a general guide to secure servers, workstations, and other network devices, in order to minimize the possibility of bypassing access controls. Each and every recommendation will not be applicable to every server, workstation, or device; therefore the system administrators should exercise their own judgment in conjunction with the requirements and business needs. The end goal is a secure server, workstation, or network device that meets the functional and business needs of BCIT.

The minimum requirements for a secure server, workstation, or network device configuration include, but are not limited to:

- Enable strong passphrases on all accounts, remove or disable default accounts or change password if default account is required.
- Remove inactive user accounts and immediately revoke access for any terminated users.
- Use “least privilege” guiding principle when assigning user access rights and permissions.
- Disable unused services.
- Use host based firewalls if available (defense in depth).
- Use “least privilege” guiding principle when configuring network or host based firewall rules.
- For management of the network devices use end-to-end encryption technology.
- Use encrypted network protocols instead of unencrypted when BCIT Personal / BCIT Confidential information is being transmitted.
- Disable any open, non-authenticated, file sharing.
- Apply latest operating system patches and ensure that all system components and software have the latest vendor-supplied security patches installed. Machines must not be connected to the network until they have had the latest security updates

Guideline

applied.
- Deploy anti-virus software on all systems commonly affected by viruses and ensure that all anti-virus mechanisms are current and actively running.
- Encrypt BCIT Personal / BCIT Confidential data or any data you consider sensitive.
- Audit the use of all privileged accounts
- Review log files regularly.
- Configure automatic clock synchronization to the IT Services common time source.

11. Inactive Accounts and Sessions Management

Cross-reference: Policy 3502 sections 6.2.2, 6.2.3

Inactive Account Management

Review accounts at least every 90 days and disable as follows:

- Accounts that have access to any BCIT Personal or BCIT Confidential information must be disabled after 90 days of inactivity or sooner
- Accounts that have access to any BCIT Internal information (but no access to BCIT Personal / BCIT Confidential information) must be disabled after 180 days of inactivity or sooner.
- Accounts that have access to only Public information must be disabled after 365 days of inactivity or sooner.

Revoke employee access rights upon termination. System access must be revoked prior to or during the termination process.

Inactive Session Management

Automated session lock mechanisms must be in place to enable locking of the information system session. The information system shall also detect inactivity and block further access until the user re-establishes the connection using proper identification and authentication processes. Also, the information system shall identify and terminate all inactive remote sessions (both user and information system sessions) automatically.

Configure information systems and applications to enable locking of the inactive sessions as follows:

Sessions that have access to:

BCIT Personal / BCIT Confidential / BCIT Internal

- Session lock: disable local access automatically after 15 minutes of inactivity (e.g. password protected screen saver). Require a password to restore local access. For teaching or meeting environment the minimum requirement is 60 minutes of inactivity (shorter is preferred). In all cases, if the information system is going to be left unattended, the session must be locked up.
- Session termination: terminate all remote sessions after 30 minutes of inactivity.

Public

- No session lock as well as no session termination is required

Guideline

12. Security Requirements in Information System Projects

Cross-reference: Policy 3502 section 7.1

Information security needs to be involved at 3 different points of information system projects:

- At the requirements phase to identify information security requirements
- At the technical design phase to ensure best security practices in the technical design
- And just prior to implementation to ensure appropriate security is in place

It is more costly to fix the later in project security is addressed. Contact ISO for assistance in these phases.

Requirements Phase

System Owners should go through BCIT Policies and Guidelines and determine what security requirements are applicable to their projects.

Technical Design Phase

Follow best security practices in the technical design where appropriate. Perform risk analysis (risk assessment) to identify threats, and implement security requirements (e.g. server placement, access controls, data encryption). See Procedure 3502 (System Risk Assessment).

Implementation Phase

Follow best security practices in the implementation to detect and remove security and privacy issues in the production. Contact ISO who will perform scans and checks of security settings for the system.

13. Technical Vulnerability Monitoring and Management

Cross-reference: Policy 3502 section 7.4

The ISO and each IT Administrator are responsible for monitoring security sources for vulnerability announcements, patch and non-patch remediation, and threats that correspond to the software within their software inventory. A variety of sources should be monitored to ensure that the ISO and IT Administrators are aware of all newly discovered vulnerabilities.

Risks should be reported to system owners who will determine acceptable risk, and take timely appropriate measures to address risks (accept, mitigate or transfer the risks).

There are several types of resources available for monitoring the status of vulnerabilities, remediation, and threats. Using more than one type of resource is recommended to ensure accurate and timely knowledge. The most common types of resources are as follows:

- Vendor Web sites and mailing lists

Guideline

- Third-party information security related Web sites, forums, and blogs
- Third-party information security related mailing lists and newsgroups
- Vulnerability scanners
- Vulnerability databases
- Patch management notifications
- Other notification tools.

Vendors are the authoritative source of information for patches related to their products. However, many vendors will not announce vulnerabilities in their products until patches are available; accordingly, monitoring third-party vulnerability resources as well is recommended.

The following resource types should be monitored at a minimum:

- Patch management notifications, to obtain all available patches from supported vendors
- Vendor security mailing lists and Web sites, to obtain all available patches from vendors not supported by the enterprise patch management tool
- Vulnerability database or mailing list to obtain immediate information on all known vulnerabilities and suggested remediation
- Third-party vulnerability mailing lists that highlight the most critical vulnerabilities (e.g., the US-CERT Cyber Security Alerts).

After initial assessment of a new vulnerability, remediation, or threat, the ISO and IT Administrators should continue to monitor it for updates and new information. For example, a software vendor might release a new patch in place of a software reconfiguration it originally recommended as a temporary remediation measure. By performing ongoing monitoring for new information, the ISO and IT Administrators would be aware of the new patch and could determine if it would provide a better solution than the software reconfiguration. Ongoing monitoring is also important because additional analysis of vulnerabilities might determine that they are more or less severe than previously thought.

General Vulnerability Management Resources

Resource Name	**URL**
US-CERT National Cyber Alert System	http://www.us-cert.gov/cas/
US-CERT National Vulnerability Database	http://nvd.nist.gov/
US-CERT Vulnerability Notes Database	http://www.kb.cert.org/vuls/
Open Source Vulnerability Database	http://www.osvdb.org/
SecurityFocus Vulnerability Database	http://www.securityfocus.com/vulnerabilities

Common Operating Systems

Guideline

Web Site or Page Name	URL
Apple	
Apple Support	http://www.apple.com/support/
Apple Downloads	http://www.apple.com/support/downloads/
Linux	
Red Hat Security Updates	https://www.redhat.com/security/updates/
CentOS Security Response Team	http://centos.org/modules/tinycontent/index.php?id=17
Microsoft	
Microsoft Download Center	http://www.microsoft.com/downloads/search.aspx?displaylang=en
Microsoft Help and Support	http://support.microsoft.com/default.aspx
Microsoft Security Home Page	http://www.microsoft.com/security/default.mspx
Microsoft Security Notification Service	http://www.microsoft.com/technet/security/bulletin/notify.mspx
Microsoft Windows Update	http://windowsupdate.microsoft.com/
Security Bulletins	http://www.microsoft.com/security/bulletins/alerts.mspx
Novell	
Novell Security	http://www.novell.com/products/security.html
Novell Support	http://support.novell.com/

14. Wireless Network Security

Topology and Configuration

The Network Team within IT Services creates and maintains documentation and diagrams covering topology and configuration of wireless networks. All wireless access point deployments must be approved by IT Services. Any access point on BCIT campuses installed without the permission of IT Services becomes rogue access point. Monitoring will be done by IT Services and rogue access points will be subject to removal. Access points must not be deployed in zones where BCIT Personal or BCIT Confidential information is stored. If a rogue access point is discovered on any of these networks, the rogue access point will be disconnected by IT Services immediately.

Physical Security

The access points should be physically secured to prevent them from any unauthorized access and physical tampering (where possible). If possible, access points should be deployed above a suspended ceiling so they are “out of sight, out of mind”, with only the antenna visible. If this is not possible and the access points are physically accessible, management via local ports should be disabled or only available via secure access methods. The access points should be physically located away from external sources of electromagnetic interference, e.g. microwave ovens. The access point should be kept in a weatherproof container if they are located in the open area.

Confidentiality and Integrity

BCIT Confidential and BCIT Personal information must not be transmitted unprotected over wireless network. The information must be encrypted prior to transmission over the

Guideline

wireless network so as to protect its confidentiality and integrity. Network or end-to-end encryption such as IPSec-based VPN or equivalent technology must be used to protect such information during transmission. Due to its vulnerabilities, the WEP and WPA encryption should not be used as the only form of protection to ensure the confidentiality and integrity of the information transmitted over the wireless network. See Guideline 3502 (Information Handling Principles).

Key Management

Any encryption keys used for encrypted wireless communication, must be protected from unauthorized access. This is to prevent any unauthorized personnel from decrypting wireless data traffic if they get hold of the symmetric encryption keys. Strong symmetric encryption, e.g. using 128-bit key length, should be used to protect the information that is transmitted over the wireless network. If shared static keys are used then the encryption keys should be changed periodically, e.g. once every 90 days. When available, dynamic keys should be used to mitigate the security risks that are inherent with the use of shared static keys, e.g. exposure or theft of static encryption keys stored in the access points and wireless stations, dictionary attack on the sniffed data traffic. The symmetric encryption keys must be protected during key distribution to the users.

User Authentication

Identity of the user must be verified and user authentication mechanisms such as users' ids/passwords and/or security tokens must be used to prevent unauthorized access to the BCIT internal networks or the Internet via the wireless network. See Procedure 3502 (Password Use).

Access Control

Network or application level access control and user authentication must be maintained to prevent unauthorized access to the BCIT wired networks and applications in the event that the security of the wireless network has been compromised. Also, access control to prevent such access to the Internet must be maintained. Access control mechanisms such as firewalls must be implemented to segregate the wireless networks from the BCIT wired networks. The wireless network must be deployed in a different network zone, which is separate from the wired networks.

Client Security

Personal firewalls must be installed and configured on the wireless station where possible to prevent and detect any unauthorized access to the wireless station over the wireless network. Network file sharing on the wireless stations should not be configured. If required then additional access protection should be in place (e.g. id/password) to prevent any unauthorized access to their local files. Software programs that can be used to configure the wireless station as an access point should be removed to minimize set-up of rogue access points. This is to prevent unauthorized access to the internal wired network via the rogue access point due to insecure configurations.

For personal wireless equipment, the owner of such equipment should:

- Install and configure personal firewall
- Disable network file sharing
- Disable ad-hoc wireless mode

Guideline

User Awareness

Where it is not required, the users should not be allowed to set up their wireless stations in ad-hoc mode and communicate with each other without going through the access point. This is to prevent unauthorized access to the user's files if they are not protected. The user should power down the wireless station when it is not being used for a long period of time, e.g. after office hours. This will reduce the risk of attacks on the wireless station over the wireless network. The user's wireless station should not have concurrent direct connection to any un-trusted network, e.g. the Internet, when the wireless station is connected to the internal wired network. This is to prevent any unauthorized access to the internal wired network via the wireless station.

Administration of Wireless Infrastructure

The built-in management ports of the access point should be disabled or password-protected to prevent any unauthorized access to the access points. All unnecessary services and ports in the access points should be removed or closed. The default SNMP community string should be changed if the access point has SNMP agent running on it. This is to prevent an attacker from reading or writing to the access point. Periodic scanning on the wireless network should be conducted to detect the presence of rogue access points, unauthorized ports/services or any security vulnerabilities in the network. The password for remote management of access points can be captured and used to gain unauthorized access to the access points. As such, administration of access points should not be done over the wireless network. Instead, the access points should be administered via the wired network using encrypted protocols (e.g. SSH, HTTPS), or locally via the access point's built-in management ports. Wireless-side management access to wireless access points and controllers should be disabled, wired-side access limited to certain IP addresses, subnets or VLANs. Vendor software updates should be frequently monitored and patches promptly applied to improve network security.

Availability

The wireless network is vulnerable to denial of service attacks such as network jamming. As such, it should not be used as the only means to access BCIT networks and systems.
Load balancing across multiple access points should be implemented to mitigate the risk of an access point being inaccessible due to flooding of network packets at a particular access point.

Logging and Audit Trails

Access to the wireless network, including unauthorized network traffic, must be logged to detect attacks directed over the wireless network. Any exceptions or abnormal network activities must be logged and alerts sent to the administrators and ISO. See Guideline 3502 (Minimum Logging Standards, Logs Retention) and Procedure 3502 (Monitoring System Use, Information Security Incident Reporting).

15. Information Security Incidents

Cross-reference: Policy 3502 section 8.1.1

The Information Security Office must be contacted if you become aware of any real or suspected breaches of information security including:

Guideline

- Unauthorized access
- Unauthorized usage of a user's account
- BCIT Personal, BCIT Confidential, or BCIT Internal information that is poorly protected
- System or network intrusions
- Information security weaknesses
- Willful damage
- Fraud relating to information security
- Theft of a device containing BCIT Personal or BCIT Confidential information
- Non-conformance to BCIT information security policies

For issues of child pornography, fraud, or physical harm, contact BCIT Safety & Security or local law enforcement.

See Procedure 3502 (Information Security Incident Reporting).

16. Establishing System Ownership

Cross-reference: Policy 3502 section 1.1.2 (System Owners)

System Owners are senior BCIT officials / managers (e.g. Vice Presidents, or their designees) within each business and/or operational unit at BCIT where the information system was created or is the primary user of that system.

If the information system is shared across business and/or operational units, BCIT Vice Presidents must decide who will be system owner for the information system.

17. Payment Card Industry Data Security Standard Compliance

BCIT will follow Payment Card Industry Data Security Standard (PCI DSS) as defined by the Payment Card Industry Security Standards Council.

Strategy

BCIT will not collect, process, store or pass cardholders data through BCIT systems. The handling of cardholders data will be outsourced to a third-party PCI DSS compliant service provider. The service provider must be fully compliant with the latest version of PCI DSS defined by the Payment Card Industry Security Standards Council.

18. Network Zones

Cross-reference: Policy 3502 section 5.6.4

Network Zone Description:
The network is broken up into logical areas (network zones) with a goal of reducing network complexity and security rules across the network. Devices with similar security requirements would reside in the same network zone allowing for security rules to apply to the entire

Guideline

network zone rather than having many rules applied to individual devices. This will reduce the number of security rules making the security architecture easier to understand, implement, and maintain.

Devices are placed in a network zone that meets their security requirements. If the security requirements of a device changes which would require opening up the security restrictions in the network zone then the device is instead moved to another network zone that meets its security requirements. Holes will not be punched in the network zone security for the device.

Security rules that allow traffic across multiple network zones should be the exception rather than the rule. Some valid uses of rules across network zones would be for a web server in the public access network zone accessing its database in a protected network zone.

In all cases security rules must use the least privilege principle. Only allow what is required and deny all the rest. For example, a web server network zone would be normally stateful, only have ports 80 and 443 open and the other ports closed.

Each network zone must have an assigned Zone Administrator who is accountable to ensure that the security characteristics of the network zone are not introduced that weakens the required security characteristics of the zone.

Network Zone characteristics:

- Provides perimeter defences for devices in the network zone
- Identifies discrete entry points
- Filters traffic at entry points
- Monitors traffic at entry points
- Is part of the overall security infrastructure along with end-system, application, and data security
- Has an assigned person accountable for the security for each network zone

Network zones provide traffic control between them to ensure that:

- Required traffic is allowed to pass between network zones
- Malicious traffic is identified and filtered wherever possible
- Traffic is directed to specified resources
- Outgoing traffic does not expose the network zone to additional risks

To manage risks associated with backdoors to the network, zones ensure that:

- All devices attached to a Network Zone are authorized;
- All interfaces with other Network Zones are authorized;
- All boundary subsystems are hardened against attack; and
- Host configuration at the perimeter is strictly controlled and appropriate assurance levels are enforced.

Perimeter defences are applied at Network Zone boundaries to ensure that sensitive assets (e.g., in the internal network zones) are maintained behind multiple layers of defences and to limit the damage associated with the failure of a perimeter defence mechanism.

Only those services available at the interface of a network zone should be visible to other Network Zones. There should be no exposure of any other network services to entities outside a Network Zone.

Guideline

The network zones will include:

- Administrative zone – for key business users and systems
- Academic zone – for faculty and students for the purposes of teaching
- Residence zone – for students in residence
- DMZ – for systems that provide services to the public (internet)
- PCI zone – for systems and devices that handle Payment Card Information
- Wireless zone – for wireless users

Network Zone documentation must be kept current and copies provided to the Information Security Officer.

Network Zone documentation should follow the format below:

Network Zone Documentation

Zone Name:	*Zone name*
Version:	*1.0*
Date:	*Date*
Zone Administrator:	*Person accountable for the security of the zone*

Purpose

What information security purpose does the network zone fulfill?
Why was the network zone created?

Zone Perimeter Defences

How is the network zone isolated? (vlans, firewall, etc.)
What is the IP range for the network zone (if applicable)?
What is the entry point(s) for the network zone?
What traffic is allowed to enter the network zone?
What traffic is allowed to leave the network zone?

Inter-Zone Relationships

What traffic is allowed to enter from what network zone?
What traffic is allowed to go to what other network zone(s)?
List any security precautions required for traffic between network zones.

Zone Guidelines

What types of devices are placed in this network zone?
How should devices in this network zone be secured?
List any other guidelines for this network zone.

Revision History

Guideline

Related Documents

BCIT Policy 3502, Information Security
BCIT Procedure 3502, Information Security
BCIT Policy 6701, BCIT Records Management

Amendment History

1. Created 2016 May 30