Information Security Procedure

Procedure No.:	3502-PR1
Version:	1
Policy Reference:	3502
Category:	Information Management
Approving Body:	Board of Governors
Executive Sponsor:	Chief Information Officer
Department Responsible:	Information Technology Services
Directory of Records:	0650-15
Approval Date:	2020 MAY 26

Objectives

This procedure applies directly to BCIT Policy 3502, Information Security. This procedure describes processes and requirements for the protection of BCIT's information assets.

Table of Contents

Who Does This Procedure Apply To?

All BCIT information and computing, communications, and networking resources connected to BCIT facilities and the users of these resources.

Other Information

None.

Procedure

1. Password Use

Cross-reference: Policy 3502 section 5.3.4

Selection:

If possible, use passphrases instead of passwords. Passphrase is a sequence of words. It is generally longer than password for added security, but is easier to remember. Passphrases meet all password complexity requirements due to the use of upper / lowercase letters and punctuation, and you can get an extremely secure password by using at least 3 words.

Passphrase example: *This is MY password!*

If you cannot use a passphrase, for example due to the length limitation or the information system does not allow spaces, follow these steps:

What to do	Suggestion	Example
Start with a sentence or two (about 10 words total).	Think of something meaningful to you.	*Long and complex passwords are safest. I keep mine secret.* (10 words)
Turn your sentences into a row of letters.	Use the first letter of each word.	*lacpasikms* (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	*lACpAsIKMs* (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	*lACpAs56IKMs* (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	*?lACpAs56IKMs* (13 characters)
Add length with symbols.	Put a symbol at the end.	*?lACpAs56IKMs"* (14 characters)

More examples:

Sentence / Passphrase = *My alarm goes off at 6:45, weekdays only!*
Password = *Mag0@6:45,w0!*

Sentence / Passphrase = *Goodbye yellow brick road, Elton John*
Password = *G00dybr,EJ*

Sentence / Passphrase = *We all live in a yellow submarine, The Beatles*
Password = *Waliay$,TB*

Sentence / Passphrase = *The pink cat jumped over 2 blue frogs!!*

Procedure

Password = *Tpcj02bf!!*

Sentence / Passphrase = *My dog Simba will be 9 years old this year*
Password = *Md$wb9y0ty*

DO NOT use any passwords / passphrases from the examples above. Create your own unique passwords / passphrases. Avoid common phrases, lyrics, or quotations; these can be easy for hackers to guess. While randomly selected words will make a stronger passphrase than words typically used together, using your random words in a grammatical English sentence will make the passphrase much easier to remember.

Use, Protection, and Management:

- Do not use BCIT passwords or passphrases for non-BCIT accounts.
- Use different passwords for different services. In particular have a unique password for banking sites.
- Change passwords regularly. If you think that someone else knows your password, change it immediately.
- Don't send your password by email. Neither HelpDesk nor any reputable firm will ask you to do this.
- Never disclose your passwords or passphrases to anyone else.
- Do not enter your password or passphrase when others can see what you are typing.
- Do not recycle passwords (e.g. password2, password3).
- Do not write passwords down. Instead, consider using password / passphrase vaulting.

Passphrase (or password) vaulting is the practice of storing many different passwords and passphrases behind a single, strong passphrase. If you have several different passwords and passphrases (e.g., for online banking, email accounts, and other secure applications), you may have difficulty remembering them when needed. Rather than compromising security by repeating passphrases among applications or by physically writing the phrases down, you can employ passphrase vaulting (e.g. a password manager) to store all the phrases behind one secure, but easily remembered, passphrase.

KeePass (http://keepass.info) is an example of a reliable and free open source password manager.

2. Clock Synchronization

Cross-reference: Policy 3502 section 4.11.6

BCIT utilizes Network Time Protocol (NTP) and Windows Time Service as the standard for clock synchronization. BCIT does not support older and simpler time protocols (TIME - port 37, DAYTIME - port 13).

Procedure

Common time source: In order to provide trustworthy time source for BCIT information system environments as well as offer redundancy, IT Services administers two internal NTP servers - ***time1.bcit.ca*** and ***time2.bcit.ca***.

Both servers are configured to synchronize to NTP servers of National Research Council (NRC). NRC is the federal agency responsible for official time, and NRC time is referred to its primary cesium atomic clocks - maintained at the NRC time standards laboratory in Ottawa.

Optional: GPS NTP server - time syncing using GPS receiver and outdoor antenna.

The GPS receiver outputs UTC (Coordinated Universal Time) date and time of day in the transmitted data. After the initial position fix, the date and time of day are calculated using GPS satellite information and are synchronized with the one-pulse-per-second output. GPS time synchronization does not require an Internet.

Access to GPS NTP server is limited to BCIT NTP servers (time1.bcit.ca, time2.bcit.ca) only.

The following table outlines the time hierarchy and configuration in BCIT network.

Servers / Workstations	Synchronize to	Protocol
BCIT NTP servers: • time1.bcit.ca • time2.bcit.ca	NRC time servers: • time.nrc.ca • time.chu.nrc.ca (Optional: GPS NTP Server)	NTP
Non-Windows computers (Linux, OSX, AIX, etc.), appliances, and other network devices	BCIT NTP servers: • time1.bcit.ca • time2.bcit.ca	NTP
Windows computers (not members of Active Directory)	BCIT NTP servers: • time1.bcit.ca • time2.bcit.ca	NTP
Server holding the PDC Emulator role in the Active Directory forest root domain	BCIT NTP servers: • time1.bcit.ca • time2.bcit.ca	NTP
Server holding the PDC Emulator role in the Active Directory domain outside the forest root domain	PDC Emulator or any domain controller from its parent domain	Windows Time Service
Domain controllers in the Active Directory domain	PDC Emulator in their domain	Windows Time Service

Procedure

Windows clients and member servers of the Active Directory domain	Domain controller with which they authenticate	Windows Time Service

Individual system administrators are responsible for ensuring proper clock synchronization. If the system does not provide automatic clock synchronization then system administrator must check and adjust the system time whenever the time is out more than 30 seconds.

If the time synchronization using NTP protocol has to be manually configured:

- Windows servers/workstations - open a command prompt and enter the following command: *net time /setsntp:time1.bcit.ca,time2.bcit.ca*
- Other operating systems, appliances, and network devices – please refer to your system's documentation

Time synchronization using Windows Time Services does not have to be manually configured. It is a built-in Windows service. Please ensure that the service is running.

3. Monitoring System Use

Cross-reference: Policy 3502 section 4.11.3

Security event is an occurrence in an information system that is relevant to the security of the system.

1. Use automated utilities to review audit records daily for unusual, unexpected, or suspicious security events and behavior. Once the anomalies are identified investigate detailed logs.
    a. Operating systems and application: review system/application log records for
        - Privileged operations, such as use of administrator accounts
        - Unauthorized access attempts
    b. Network devices: review network log records for
        - Unauthorized use of network equipment or network protocols
        - Unauthorized access attempts
        - Network scans from inside or outside of BCIT
        - Intrusion detection alerts
        - Bandwidth utilization rates and denials of service (DoS, DDoS)
        - Number of network protocol transactions occurring in a certain period, such as increased SMTP traffic from or to the systems where such traffic is not expected
    c. Inspect administrator groups regularly to ensure unauthorized administrator accounts have not been created.
2. Perform manual reviews of logs or privileges randomly once per month:
    a. To ensure the automated utilities and scripts are working correctly.
    b. For additional information in the logs that should be monitored.

Procedure

Increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to BCIT operations and assets.

4. Mobile Device Security

Cross-reference: Policy 3502 section 4.4

1. Configure mobile devices to be secure where possible:
   a. Enable auto-lock (idle timeout, screensaver timeout, etc).
   b. Enable password protection and require complex passwords.
   c. Avoid using auto-complete features that remember user names or passwords.
   d. Enable remote wipe if available. If the device is stolen or lost it can be wiped remotely.
   e. Ensure that SSL or VPN protection is enabled if available to ensure the Protectedity of the information transmitted over the wireless or any unsecure network.
2. Connect to secure Wi-Fi networks and disable Wi-Fi when not in use:
   a. Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi. It will minimize the exposure of the device to attacks utilizing such features.
   b. Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices. It will minimize the exposure of the device to attacks utilizing Bluetooth connection.
   c. Avoid joining unknown Wi-Fi networks. If you have to join such network (e.g. Wi-Fi network at the airport or coffee shop) ensure that SSL or VPN protection is enabled (e.g. connect to BCIT VPN)
3. Update mobile devices frequently. Select the automatic update option if available.
4. Utilize anti-virus programs and configure automatic updates if possible.
5. Use an encryption solution to keep data on portable device secure.
6. Take appropriate physical security measures to prevent theft or enable recovery of mobile devices:
   a. For laptops, use cable locks.
   b. Use tracing and tracking software if possible.
   c. Never leave your mobile device unattended.
   d. Report lost or stolen devices immediately to Safety & Security.
   e. Remember to back up data on your mobile device on a regular basis.
7. Securely wipe all information stored in a device prior to discarding, exchanging, or donating it.

5. Disposal and Reuse of Media and Hardcopy

Cross-reference: Policy 3502 sections 4.8.2, 4.8.3

All IT Services issued devices must be returned to IT Services for disposal (see Policy 3502 regarding Assigning Asset Custodians).

Disposal of Paper Records

For disposal of transitory paper records use the locked Recall containers located across BCIT campuses. Contact the Records Management Office at RMO@bcit.ca to

Procedure

arrange for secure destruction of records in accordance with the BCIT Directory of Records Classification and Retention Schedules.

Disposal of CDs, DVDs and Blue-Ray Disks

Bring the media to IT Services (Service Desk). IT Services will ensure that the media will be kept secure until IT Services destroy the media.

Hard Drives, Compact Flash Drives, SD Cards, USB keys, Floppy Disks, Zip Disks

Bring the device to IT Services (Service Desk). IT Services will ensure that the device will be kept secure until IT Services performs a security data wipe and coordinates the disposal with Materials Management.

PDAs, BlackBerries and Cellular Telephones

If available, use utilities coming with the device to securely wipe all information and return to IT Services (Service Desk) where a full manufacturer's reset to factory default settings will be performed.

6. Persons Giving Information Over the Telephone

Cross-reference: Policy 3502 sections 4.9.3

Always be careful about disclosing information that has been designated as Protected Information.

The disclosure of Personal Information must be only for a purpose authorized under the Freedom of Information and Protection of Privacy ("FIPPA") and Policy 6700, Freedom of Information and Protection of Privacy. Requests from third parties for disclosure of Personal Information must be made in writing, identifying the information sought, the authority for the request and the request.

Before providing any information over the telephone, you must verify the identity of the caller. Check the identity of the caller (as applicable, their full name, BCIT ID number, date of birth) and if in doubt, call back where possible, using their phone number on file.

If you're unsure or unable to verify a caller's identify, do not disclose any Protected or Personal Information. Pass on the call to your manager or consult with the Privacy Office at privacy@bcit.ca or the Director, Safety, Security and Emergency Management.

If you have to give Personal Information or Protected Information, provide only what is necessary for the task at hand and be aware of others who may be listening

Telephone

- When providing Personal Information or Protected Information ensure that unauthorized persons cannot overhear the information (e.g. close the door, move to another room, etc.)
- Before providing Personal Information or Protected Information, confirm that you have the correct phone number for your intended recipient.

Procedure

- If you use pre-programmed phone numbers, regularly check to ensure that the phone numbers are accurate and up to date.

If you have been called to provide the information that is classified as Personal Information or Protected Information, be cautious.

- If the information system allows security questions for the user identity verification (e.g. security questions in Banner), use the questions to verify the caller's identity.
- If the information system does not allow security questions:
    - For external phone numbers: check out any caller by requesting written request (e.g. mail, email, fax) for the information, a call back number, references and time to think over their request. If the person has a registered phone number with BCIT, use this phone number to call back.
    - For internal phone numbers: ask for name and use phone number from BCIT Phone Directory to call back.

Fax

- Any fax machine used to send or receive Personal Information or Protected Information should be located in a place that prevents unauthorized persons from seeing faxed information. Access to the machine should be controlled.
- Always use a fax cover sheet. The cover sheet should clearly identify the sender (with call-back particulars for the sender) and the intended recipient. It should specify the total number of pages being sent.
- Before you fax Personal Information or Protected Information, confirm that its recipient has taken appropriate precautions to protect the information upon receipt.
- Before faxing Personal Information or Protected Information, confirm that you have the correct fax number for your intended recipient.
- If you use pre-programmed fax numbers, regularly check to ensure that the fax numbers are accurate and up to date.
- After you have dialed a fax number, carefully check the number you dialed before sending the fax. This also applies when using pre-programmed fax numbers.
- You should check each fax confirmation report at once to be sure the fax went to the right place -- check the number on the report against the recipient's number. Also check the number of pages actually transmitted and received.
- Retrieve material you are sending by fax from the fax machine as soon as it has been processed for sending. Do not leave it sitting on or near the fax machine. When you are faxing Personal Information or Protected Information, stay by the machine at all times during faxing.
- If you must fax Personal Information or Protected Information, phone first to confirm that the intended recipient is actually the right person to receive the fax to confirm, that the recipient will be there to receive the fax, and to confirm the recipient's fax number. Ask the intended recipient to call to confirm receipt of the fax.
- If you receive a fax in error, promptly notify the sender and destroy the information, as requested by the sender.
- When receiving a fax, check the number of pages you have actually received against the number of pages noted on the fax cover sheet. Check to ensure you have not received any material you should not be getting. If you do receive

Procedure

material you should not be getting, promptly notify the sender and return or destroy the information, as requested by the sender.

- If you fax Personal Information or Protected Information, consider using secure fax machines that employ encryption or other security measures. If your fax machine has a feature that requires the recipient to enter a password before the recipient's machine will print the fax, use that feature for sensitive personal information at least. Similarly, the recipient could arrange for the sender to make sure the recipient must supply a password to retrieve faxes of Personal Information or Protected Information.
- Do not make or keep more copies of faxed or emailed material than you truly need. Securely destroy extra copies (see section 5).
- If someone asks you to fax their personal information to them, first explain to them how faxing risks their Personal Information being accidentally disclosed or deliberately intercepted by other people and get their consent before you fax or email their Personal Information.

7. Information Assets with Configurable Security Characteristics

Cross-reference: Policy 3502 (System Owners, IT Administrators)

System Owners must specify security requirements for the configurable Information Asset. IT Administrators must ensure the asset is configured properly to meet the security specifications required by the System Owners.

System Owners must maintain a list of all configurable IT Assets in their scope of administration. Anytime a configurable IT Asset comes into their scope of administration, the System Owners must ensure there is a designated IT Administrator for that asset, and must add the asset and its designated IT Administrator to the list.

The list must unambiguously identify the IT Asset and its designated IT Administrator. The list must be reviewed regularly.

Assigning IT Administrators
The System Owner of each information system must ensure there is an IT Administrator for each asset comprising the system. Such administrator must be able to perform tasks and duties which might include:

- Analyzing system logs and identifying potential issues with computer systems;
- Introducing and integrating new technologies into existing data center environments;
- Performing routine audits of systems and software;
- Performing backups;
- Applying operating system updates, patches, and configuration changes;
- Installing and configuring new hardware and software;
- Adding, removing, or updating user account information, resetting passwords, etc;
- Answering technical queries;
- Responsibility for security;

Procedure

- Responsibility for documenting the configuration of the system;
- Troubleshooting any reported problems;
- System performance tuning; and
- Ensuring that the network infrastructure is up and running.

A secondary IT Administrator must be assigned to assist and backup the primary IT Administrator. The secondary IT Administrator should have the same authority and access rights to the information system as the primary IT Administrator.

8. User Authentication for External Connections

Cross-reference: Policy 3502 section 4.7.2

The following are technologies approved for the remote access to BCIT networks:

- AccessAnywhere
- AppsAnywhere

AccessAnywhere
BCIT VPN (i.e. AccessAnywhere) provides a secure connection to the BCIT network. This enables staff to access network resources from outside the BCIT network (e.g. from home). To use BCIT network resources (such as mapped folders, applications and printers) you must use AccessAnywhere.

How to request access to AccessAnywhere:

- https://helpdesk.bcit.ca/fsr/network/748.html

How to log on to AccessAnywhere:

- Windows: https://helpdesk.bcit.ca/fsr/network/743.html
- MacOSX: https://helpdesk.bcit.ca/fsr/network/756.html

AppsAnywhere
AppsAnywhere is a service that allows access to software provided by BCIT, and the BCIT network resources via that software. All the software runs on servers in BCIT data center.

How to use AppsAnywhere:

- https://helpdesk.bcit.ca/fsr/sr/appsanywhere/757.html

Other technologies
If there is a request for remote access that cannot be provided by either AccessAnywhere or AppsAnywhere, and the access can be provided by some other technology, the request must be approved by the IT Services and Information Security Officer (ISO).

Authorization requests must first be submitted for approval via the HelpDesk Incident Monitor to IT Services, the network team in Technical and Infrastructure Services. Once approved by the network team, the request will be forwarded to the Information Security Officer, who will notify the requestor of approval or rejection, and if rejected, of the reasons. The minimum lead-time for submissions is 5 business days.

Procedure

Authorization request should follow the format below:

Type:	*Type of the remote access (e.g. SSL VPN, IPSEC VPN, etc.)*
Requestor:	*Person requesting the remote connection (must be a BCIT employee)*
Administrator:	*Person accountable for the administration of the remote access*
Contact Information:	*Phone number and email of the remote access administrator*
Network Zone:	*A network zone where the remote access is requested to*

Purpose

Why the request should be approved?
Why the standard BCIT remote access cannot be used?
What business needs will the remote access fulfill?

Remote Access Description

Protocols and encryption used by the remote access application.
Will the remote access connection be initiated from the BCIT network or from the remote network?
Will the remote access connection be opened on-demand or permanent remote access is required?
What ports need to be open on the BCIT firewall?
List of IP addresses, subnets, and/or ports involved on the BCIT side.
List of IP addresses, subnets, and/or ports involved on the remote side.

Duration

Permanent or Temporary?
If temporary, provide "from" and "to" date/time, i.e. how long the remote access to the BCIT network will be required.
If permanent, provide the "from" time.

The network team or ISO may require additional information.

Procedure

9. Connecting to BCIT Network

Cross-reference: Policy 3502 section 4.7.5

Network equipment must not be connected to BCIT networks without approval from IT Services.

Authorization requests must be submitted via Service Desk to IT Services for approval. If the request is either approved or rejected, the requestor will be notified about the approval or the reason of rejection. Please note that the minimum lead-time is 5 business days.

Authorization request should follow the format below:

Type:	*Type of the network device (e.g. router, access point, etc.)*
Requestor:	*Person requesting the connection of the network device*
Administrator:	*Person accountable for the administration of the device*
Contact Information:	*Phone number and email of the device administrator*
Network Zone:	A *network zone where the device will be connected to*

Purpose

Why the request should be approved?
What business needs will the device fulfill?
What network services does the device provide?

Duration

Permanent or Temporary?
If temporary, provide "from" and "to" date/time, i.e. how long the device will be connected to the BCIT network.
If permanent, provide the "from" time.

The network team may require additional information.

Once discovered, any network equipment connected to BCIT networks without approval from IT Services will be immediately disconnected by IT Services.

10. Servers Accessible from External Networks

Cross-reference: Policy 3502 section 4.7.9

All servers that are accessible to an external network (including the Internet) must receive permission from the Cyber Security Officer (CSO).

Procedure

Authorization requests must be submitted via the IT Service Desk. Once approved by CSO, the request will be forwarded to the network team in Enterprise Technology team. If the request is either approved or rejected, the requestor will be notified about the approval or the reason of rejection. Please note that the minimum lead-time is 5 business days.

Authorization request should follow the format below:

Server Name: *Server name*
IP address: *IP address of the server*
Requestor: *Person requesting the permission for the server*
Administrator: *Person accountable for the administration of the server*
Contact Information: *Phone number and email of the server administrator*
Network Zone: A *network zone where the server will be located*

Purpose

Why the request should be approved?
What business needs will the server fulfill?
What services does the server provide?
Who is the user for that service?

Network Requirements

What ports need to be open on the BCIT firewall?
Is the access to the server required from the specific IP addresses only? If yes, provide the list of the IP addresses.

Duration

Permanent or Temporary?
If temporary, provide "from" and "to" date/time, i.e. how long the device will be connected to the BCIT network.
If permanent, provide the "from" time.

The CSO as well as the network team may require additional information.

11. Assigning Asset Custodians

Procedure

Cross-reference: Policy 3502 sections 1.1, 3.2.2

IT assets must be tracked in the IT Service's Asset Management System at each point of the lifecycle of the asset.

Acquiring IT Assets
IT assets must be purchased through Supply Management's procurement process and received through Central Stores. IT assets not tagged with a BCIT asset tag by the vendor will be assigned BCIT asset tag identifier and recorded in the IT Service's Asset Management System. Vendors who pre-tag IT assets prior to shipment to BCIT will provide IT Services with asset information including BCIT asset tag identifier prior to shipment to Central Stores.

IT assets will be deployed to and assigned to an asset custodian by IT Services.

The Asset Custodian:

- is responsible for the asset and will return the asset to IT Services on request;
- will provide IT Services with any changes in asset information; and
- will provide IT Services access to the IT asset on request

IT Services staff will confirm asset information and update information as required.

Decommissioned IT Assets - Obsolete
Asset Custodians of IT assets that are considered technologically obsolete, operationally inefficient, or surplus and no longer required by the custodian, must return the IT asset to IT Services for redeployment or disposal. IT Services will assume custodianship of the asset and perform a security data wipe on the IT asset prior to redeployment or disposal.

Decommissioned IT Assets - Employee Leave of Absence
An employee on a leave of absence will surrender the IT asset as follows:

If the position is being backfilled:

- The employee's manager will retain custody of the IT asset until the position is filled.
- IT Services will arrange for a security data wipe and render the computer inoperative.
- The manager will inform IT Services when the new employee has arrived and has assumed custodianship of the IT asset.
- IT Services will install and configure a suitable software image for the new employee's use.

IT Services will arrange for a security data wipe and render the computer inoperative.
If the position is NOT being backfilled and the length of the leave is greater than 3 months:

- The employee's manager will arrange for the IT asset to be surrendered to IT Services. IT Services will assume custodianship of the asset and perform a security data wipe on the IT asset prior to redeployment or disposal.

If the position is NOT being backfilled and the length of the leave is less than 3 months:

Procedure

- The IT asset custodian is responsible for securing the asset

Decommissioned IT Assets - Employee departure
When IT Services is notified by Human Resources of an employee's departure, IT Service's will provide the employee's manager a list of IT assets assigned to that employee. The manager will confirm the list of IT assets and assume custody of those assets.

The employee's manager will consult with IT Services regarding retention of locally saved institute data prior to security data wipe.

If the vacated position is going to be filled within 3 months:

- The employee's manager will retain custody of the IT asset until the position is filled;
- IT Services will arrange for a security data wipe and render the computer inoperative;
- The manager will inform IT Services when the new employee has arrived and has assumed custodianship of the IT asset; and
- IT Services will install and configure a suitable software image for the new employee's use.

If the vacated position is not going to be filled within 3 months:

- The employee's manager will arrange for the IT asset to be surrendered to IT Services; and
- IT Services will assume custodianship of the asset and perform a security data wipe on the IT asset prior to redeployment or disposal.

12. Delegating Accounts through Controlled Sharing

Cross-reference: Policy 3502 sections 5.3.1, 5.3.4

Password must not be shared with any other person at any time. The only exception is when the system does not provide the ability to delegate. In such case the following steps must be followed:

1. User A (i.e. who delegates) changes his or her password.
2. User A gives his or her new password to User B (i.e. who is delegated).
3. User B immediately changes the User A's new password.

At this point, User B has the custody of User A's ID and password. User A does not know the new password and cannot use his or her account. Any action taken henceforth by User A's ID was taken by User B.

In order to return the credentials, the opposite steps must be followed:

1. User B (i.e. who was delegated) changes the User A's password.
2. User B gives the new password to User A (i.e. who delegated).
3. User A immediately changes his or her password.

Procedure

At this point, User A has the custody of his or her ID and password. User B does not know the new password anymore and cannot use the User A's account. Any action taken henceforth by User A's ID was taken by User A.

Both sides (User A and User B) should log and keep the records when they handed the password over and received it back.

13. Short Term Accounts

Cross-reference: Policy 3502 section 5.3.2

Special users, third party contractors, adjunct instructors, temporary employees, volunteers, or consultants having access to BCIT computing assets, networks, or telecommunications systems should be identified as such in their user names and must follow the same information security rules as BCIT students and employees with the following exceptions:

- Accounts must be deactivated, but not necessarily deleted, or the password must be changed at the conclusion of the temporary account users contract.
- Temporary account users will be given access only to those BCIT computing resources required to do their jobs.
- Generic name account may be only assigned to one user at time. Logs must be kept of the time when such account was assigned and to whom it was assigned.

14. Terms and Conditions of Employment

Cross-reference: Policy 3502 section 2.1.3

All employees must sign an application stating they agree to adhere to the policies and procedures outlined in BCIT Policy 3501 (Acceptable Use of Information Technology) and BCIT Policy 3502 (Information Security).

Such agreement must be included in the employment contract, so that employees must sign that they have read, understand and acknowledge receipt of the Policy 3501 and Policy 3502. It must be signed prior to receiving access to any BCIT account.

Furthermore, for any access agreements/applications to BCIT information systems, the agreements/applications must contain a statement that by signing the application, the applicant agrees to adhere to the policies and procedures outlined in BCIT Policy 3501 and BCIT Policy 3502.

15. Control of Non-conforming Systems

Cross-reference: Policy 3502 section 10

Exceptions to BCIT Policy 3502 may be permitted in instances where the security risk is likely to exist for more than three (3) months and a risk analysis has been performed that identifies the risk as a high-level risk to the Institute. The risk analysis must be documented by a written risk assessment (see Information Security Risk Assessment Form) and a non-

Procedure

compliance report prepared jointly by the responsible business owner, data owner, business process owner, and/or system administrator.

The non-compliance report and requests for exception must include:

- A valid business justification;
- A risk analysis;
- Compensating controls to manage risk (mitigation); and
- Technical reasons for the exception.

For all BCIT Policy 3502 exemption requests, the Cyber Security Office reviews the reports and keeps records of non-conforming systems. System Owners by approving the exemption accept the security risk caused by the exemption.

Requests for exception that create significant risks without compensating controls will not be approved. Requests for exceptions are reviewed for validity and are not automatically approved.

System Owners must periodically review requests for exceptions every six (6) months to ensure that assumptions or business conditions have not changes. If changes can be made to make the system conforming then it is strongly encouraged to do so.

16. Information Security Incident Reporting

Cross-reference: Policy 3502 section 7.1.1

Cyber Security Officer should be contacted by ITS Service Desk. If the situation is deemed an emergency and the Cyber Security Office cannot be reached, contact IT Service Desk general line. The Service Desk will notify the Cyber Security Office of the reported security incident. The Helpdesk will take no additional action unless requested by the Cyber Security Office. Wait for further instructions from the Cyber Security Office.

When reporting a security incident please provide the following information:

- Full name
- Email or phone number
- Are you affiliated with BCIT?
- Type of report:
    - Unauthorized access
    - Personal Information and/or Protected Information, that is poorly protected
    - System or network intrusions
    - Information security weaknesses
    - Willful damage
    - Fraud relating to information security
    - Theft of a device containing Personal Information or Protected Information
    - Non-conformance to BCIT information security policies
    - Other
- Precise description of the activity you are reporting

Procedure

Anonymous reports will only be investigated if evidence is provided that substantiates the report.

Please provide the following additional information if known:

- BCIT IP address(es) or hostname(s) involved
- Start and end times of activity (including time zone)
- Log excerpts showing the activity
- Any additional information (network protocol used [e.g. TCP, UDP, ICMP], port numbers, number of packets involved, operating systems, etc.)

17. Wireless Network Access

There are two SSID's available in BCIT's wireless network – "BCIT" and "eduroam". The "BCIT" SSID is clear text and the "eduroam" SSID is encrypted. The student or guest roles can use either SSID.

BCIT employees, when using wireless access at BCIT campuses, must use encrypted wireless network identified by SSID "eduroam" in order to access the administrative part of the network directly. If an employee uses unencrypted "BCIT" SSID, they must use BCIT VPN (i.e. AccessAnywhere) for the access to the administrative part of the network.

Access via AppsAnywhere is encrypted, and either "eduroam" SSID (preferred) or "BCIT" SSID can be used.

How to configure wireless access through "eduroam" network:

- Windows XP: https://helpdesk.bcit.ca/fsr/sr/wireless/770.html
- Windows 7: https://helpdesk.bcit.ca/fsr/sr/wireless/781.html
- MacOSX: https://helpdesk.bcit.ca/fsr/sr/wireless/773.html

How to log on to BCIT VPN (AccessAnywhere):

- Windows: https://helpdesk.bcit.ca/fsr/network/743.html
- MacOSX: https://helpdesk.bcit.ca/fsr/network/756.html

18. Backups

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.

Procedure

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 backup followed by incremental 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; and
- All backup data is copied to physical tape and sent offsite twice weekly.

19. Use of Voicemail

BCIT provides voice mail messaging to its faculty and staff for internal business purposes. Members of the BCIT community should limit their use of the system to this purpose. Users should not share personal voice mailboxes due to privacy reasons.

Setting up Voice-mail Greetings

- Replace the information in square brackets below with your particulars. Optional information is in parentheses. If you have a BCIT supplied cell phone include the optional information in your greeting. Repeat the cell number twice slowly.
- When specifying absences state the date of your return as opposed to the last date of your absence.
- If you specify a period of applicability in your message (e.g. for the week of Oct 15th), remember that you have made an implied commitment to keeping this information up to date. If you have trouble keeping your greeting up to date then better to omit the period of applicability.
- If you are out of the office and unreachable specify an alternate contact. Make sure this person will be available throughout the period of your absence.

Procedure

Voicemail Greeting (In the Office)
This is [your name] of [your department] (for the [period of]) I am in the office but not able to take your call. (My hours of work are [hours of work].) Please leave me a detailed message and I will return your call as soon as possible. (If your call is urgent please contact me on my cell at [my cell number -- repeat twice]) Thank You.

Voicemail (Extended Absence)
This is [your name] of [your department] (for the [period of]). I will not be in the office from [from date] returning on [return date]. During this time I will not be checking for messages. In my absence please contact [person acting for me] at [telephone number of acting person]. If your call can wait until my return, please leave me a detailed message. Thank You.

Voicemail (If Away from Office but Calling Semi-regularly in for Messages)
This is [your name] of [your department] (for the [period of]). I will not be in the office from [from date] returning on [return date] but will be checking in for messages. Please leave a detailed message and I will return your call later today. (If your call is urgent please contact me on my cell at [my cell number -- repeat twice]). Thank You.

Forms Associated With This Procedure

Information Security Risk Assessment Form

Amendment History

			Approval Date	Status
1.	Creation:	Procedure 3502-PR1 version 1	2020 MAY 26	In Force

Scheduled Review Date

2025 MAY 26