THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U1
Security Classification of UBC Electronic Information and Services

1. Introduction

1.1 UBC Electronic Information used by Users has varying degrees of sensitivity which have corresponding levels of risk and protection requirements; therefore, it is necessary to classify this information to ensure it has the appropriate level of protection.

1.2 UBC Electronic Services have varied risk based on their confidentiality, integrity and availability requirements to University operations and the volume and nature of the UBC Electronic Information they process; therefore, it is necessary to classify services to ensure they have appropriate level of protection.

1.3 This standard explains how UBC Electronic Information and UBC Electronic Services are risk classified.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

1.5 This standard applies to all UBC Electronic Information and UBC Electronic Services.

2. Information Security Risk Classification Model

2.1 UBC Electronic Information is classified as follows:

Definition	Examples	Potential Impact of Loss
Low Risk Information		
UBC Electronic Information that would cause minimal harm if disclosed, or may be freely disclosed	• Names and work contact information of UBC faculty and staff members • Information that is posted on our public website • Research information of a non-personal, **non-proprietary** nature	Minor embarrassment, minor operational disruptions
Medium Risk Information		
UBC Electronic Information that is not protected by law or industry regulation from unauthorized access, use or destruction, but could cause harm to UBC or others if released to unauthorized individuals	• Proprietary information received from a third party under a non-disclosure agreement • Restricted circulation library journals • Confidential financial information and records • Information that could allow somebody to harm the security of individuals, systems or facilities • Research information of a non-personal, **proprietary** nature	Reputational and financial impact, loss of priority of publication, loss of access to journals and other copyrighted materials
High Risk Information		
UBC Electronic Information that must be protected by law or industry regulation from unauthorized access,	• Personal Information, which must be protected under the BC *Freedom of*	Moderate harm to one or more individuals, identity theft, impact to University reputation or operations, financial loss, such as regulatory

Definition	Examples	Potential Impact of Loss
use or destruction, and could cause moderate harm if disclosed	*Information and Protection of Privacy Act* (FIPPA), including: ○ Full face photographic images ○ Student name ○ Student or Employee ID ○ Student grades ○ Home address • Payment Card Industry (PCI) Information, which must be protected under the Payment Card Industry – Data Security Standard (PCI-DSS) (e.g. credit card numbers, names, expiry dates or PINs)	fines and increased credit card transaction fees
Very High Risk Information		
UBC Electronic Information that must be protected by law or industry regulation from unauthorized access, use or destruction, and could cause significant harm if disclosed	• Social Insurance Number (SIN) • Official government identity card (e.g. Passport ID, Driver's License No.) • Bank account information (e.g. direct deposit details) • Personal Health Information (PHI) • Biometric data • Personally identifiable genetic data • Date of Birth (DoB)	Significant harm to one or more individuals, identity theft, severe impact to University reputation or operations, financial loss, such as regulatory fines or damages from litigation

2.2 The classification of UBC Electronic Information may change over time. For example, unpublished research data may be classified as Medium Risk, but after publication, it may change to Low Risk.

3. Electronic Service Risk Classification Model

3.1 Factors to consider when assessing the risk of an Electronic Service include:

3.1.1 Reputational harm

3.1.2 Financial losses

3.1.3 Number of affected Constituents

3.1.4 Volume of High or Very High Risk Information

3.1.5 Operational impact

3.2 UBC Electronic Services are classified as follows:

Definition
Low Risk Electronic Service
Loss of confidentiality, integrity or availability in a Low Risk Electronic Service would cause minimal impact to UBC's mission, safety, finances or reputation. The incident will display one or more of the following characteristics and no characteristics of higher risk classifications: • Potential financial losses could easily be funded through departmental operating funds; • Negligible effects on UBC or departmental operations; • Affects only some or no members of one group of Constituents if confidentiality breached; or • No (one day or less) negative impact on public perception.
Medium Risk Electronic Service
Loss of confidentiality, integrity or availability in a Medium Risk Electronic Service would cause minor impact to UBC mission, safety, finances, or reputation. The incident will display one or more of the following characteristics and no characteristics of higher risk classifications: • Potential financial losses could be covered with departmental funds but would significantly impact financial position; • Normal administrative difficulties experienced; • Affects only one group of Constituents, is unlikely to impact the entire group and impacts are not significant if confidentiality breached; or • Very brief (one week to six months) negative impact on UBC public perception.
High Risk Electronic Service
Loss of confidentiality, integrity or availability in a High Risk Electronic Service would have a significant business impact to one or more portfolios, but not the whole University. The incident will display one or more of the following characteristics and no characteristics of higher risk classifications: • Potential financial losses would require funding from contingency funds, the department would have no ability to cover, but the University could cover without significant impact (e.g. $500,000 to $5 million); • Delay to accomplishing UBC objectives resulting is short term non-routine measures to mitigate; • Major impact with medium-term (six months to one year) harm to a significant membership (25% or more) of one or more Constituents, if confidentiality breached; or   ○ Significant harm to a small Constituent group; • Medium term (six months to one year) negative impact on UBC public perception; or • Non-compliance with contractual requirement to maintain availability.
Very High Risk Electronic Service
Loss of confidentiality, integrity or availability in a Very High Risk UBC Electronic Service would have a major business impact to the University. The incident will display one or more of the following characteristics: • Financial losses are major and would impact the University's ability to execute its strategic plan; • Major disruption resulting in medium term (six months to one year) non-routine measures before UBC objectives can be met; • massive impact with long-term (more than one-year) harm to most of one or more Constituents if confidentiality breached; Massive impact with long-term damage to UBC public perception;

Definition
• Impact to life safety; • Non-compliance with statutory or regulatory requirement to maintain availability; or • National security implications. These systems transact or store any of the following: • High and Very High Risk Information of most members of internal constituents (student, faculty, staff, alumni); • high volumes of research information pertaining to external constituents/research subjects; or • contractual document or intellectual property of significant sensitivity. All IT infrastructure that is critical to the operations of the University falls into this category.

4. Responsibilities

4.1 The Information Steward/Owner is responsible for determining the information security classification based on the definitions and examples in the table above. Based on other relevant factors, information may be classified at a higher level than indicated above, but not at a lower level.

4.2 The Administrative Head of Unit is responsible for ensuring completion of an inventory and classification of UBC Electronic Services under their control using the Electronic Services Risk Classification model. This must be recorded in the enterprise asset inventory system, if it is available.

4.3 The Administrative Head of Unit is responsible for knowing the types of UBC Electronic Information under their control, its information security classification and where it is stored. In order to comply with our legal obligations, it is recommended that the Administrative Head of Unit keep an inventory of types of records that contain High Risk and/or Very High Risk Information. At a minimum, the inventory should contain the type of information, description and storage location. Refer to the sample inventory attached to this standard. This responsibility may be delegated to the Information Steward/Owner.

4.4 For UBC Electronic Services classified as Very High Risk, the Administrative Head of Unit is responsible for having documented assurance of compliance with the Information Security Standards. This is usually attained by sourcing Security Threat Risk Assessments at various stages in the information systems lifecycle (implementation, significant change, retirement).

5. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

BC Freedom of Information and Protection of Privacy Act (FIPPA)

What is Personal Information? [Privacy Fact Sheet]

Sample Inventory

Case Studies

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U2
Passphrase and Password Protection

1. Introduction

1.1 This document defines standards for the creation and use of passphrases and passwords to protect the UBC Electronic Information that Users handle.

1.2 Passphrases (sequences of words or other text) and passwords (words or strings of characters) are common and important ways to access and protect digital information on or off the Internet through almost any type of Device. Consequently, attackers attempting to access information use a variety of tools to guess or steal passphrases/passwords.

1.3 In summary, the top three ways to keep a passphrase/password safe and protect the information are:

1.3.1 create a strong passphrase/password;

1.3.2 guard it carefully (e.g. don't share it or write it down); and

1.3.3 avoid reusing it for other systems.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Creating a Passphrase/Password

2.1 Use a passphrase with a minimum of 16 characters. If a minimum of 16 characters is not technically allowed by a system, use a complex password that contains upper and lower case letters, numbers and symbols that is as long as possible, but a minimum of 10 characters. Guidelines for consideration:

Bad Examples (Easy to Guess)	**Good Passphrase Examples** (Preferred)	**Good Complex Password Examples**
Pa$5w0rd!	pass turtle phrase	Hx%2Pe2fWE
WhiteCaps2018	trophy.sky.sings.gold	5vE@Pu57^j
12345678ABC	1plusfourbeaches	9#fAaXu7y6tt
GameofThrones	facelessdragonhorse	p39&k1WX3EGxKo
Vanc0uv3r	rainbeachpuddles	gqEWep8#32v2xF8i
2March1976	SingingLionorLamb	Yy6*&u22rB
qwerty1234	Elephantkickscat!.!	Jb06MTKS35
M0nk3yABC	MonkeyPatsTiger1	854Htt8EvR
ILoveYou	mammamialetmego	4Qz7cSPgdAB15wLm

2.1.1 To create a passphrase, consider using a phrase of disconnected words that you can picture in your head (e.g. "plug in sunshine thimbles" or "StingersSingPaint").

2.1.2 To create a complex password when a passphrase is not an available option, consider using the first letter of each word in a phrase. For example, "I ride my bike to school at 7 AM!" becomes "Irmbtsa7AM!".

2.1.3 Avoid using a password that replaces a letter with a number, such as "Br0adcast!" where the "O" is replaced with a zero. Password guessing programs can easily crack these types of alpha/numeric replacements.

2.1.4 Password generation and storage programs should be used to create and manage passphrases/passwords.

2.1.5 Name, username, address, date of birth, family members' names or any other term that can be easily guessed should not be used to create a passphrase/password.

3. Changing a Passphrase/Password

3.1 Passphrases/passwords for Campus-wide Login accounts must be changed annually. For all other accounts, it is recommended that passphrases/passwords be changed annually. When changing a passphrase/password:

3.1.1 do not use the 10 most recent passphrases/passwords that have been used on the same system;

3.1.2 do not use the same passphrase/password for personal accounts and university accounts; and

3.1.3 it is recommended to use unique passphrases/passwords for different accounts, so that even if one is stolen, it does not allow access to other accounts owned by the same User.

Case Study: Why You Shouldn't Share Your Password

A single user ID and password was shared amongst a research lab's personnel. One of these individuals maliciously destroyed some of the data in the account. Since this was a shared account, it was challenging to identify the responsible party.

3.1.4 each time a passphrase/password change or reset occurs, a Multi-Factor Authentication (MFA) challenge is required for employee Campus-wide Login accounts. For all other accounts, it is recommended.

4. Protecting a Passphrase/Password

4.1 If a passphrase/password is written down, it must be locked away in a secure, inaccessible location such as a safe.

4.2 Best practices state that passwords should not be shared for any reason—even with trusted individuals such as supervisors or University IT Support Staff.

4.3 University IT Support Staff will never ask for Users' passphrases/passwords.

4.4 Do not respond to emails or phone calls requesting passphrases/passwords and Multi-Factor Authentication (MFA) passcodes, even if they appear to be from a trusted source. These requests are often attempts to steal Users' credentials.

4.5 Passphrases/passwords must be immediately changed if there are suspicions that they could have been compromised and the incident must be reported to UBC Information Security (see the Reporting Information Security Incidents standard).

4.6 Use of a Password Safe/Manager is the recommended method to securely store multiple passphrases/passwords, as it is only necessary to remember a single master password. Refer to the Password Safe guideline.

5. Passphrases/Passwords for Devices with Touchscreen Interfaces

5.1 Due to smartphones and tablets having touch-screen interfaces, it is not practical to use a strong password to lock the Device. Instead, a numeric password/PIN can be used, as long as it is at least five characters long.

5.2 See the Securing Computing and Mobile Storage Devices/Media standard for further requirements regarding Mobile Device security.

Choosing your Password/PIN for a Mobile Device

A simple password/PIN option is to think of a 5 or 6 letter word and spell it out using the letters on the numeric key pad. Example: HOUSE becomes "46873".

6. Biometric Alternatives to Passphrases/Passwords/PINs

6.1 Biometric controls such as fingerprint readers and facial recognition are acceptable alternatives to passphrases/passwords/PINs.

7. Multi-Factor Authentication

7.1 Where available, it is recommended that Users take advantage of Multi-Factor Authentication.

8. Additional Requirements for University IT Support Staff

8.1 For University IT Support Staff, there are additional requirements around the storage of passphrases/passwords. These requirements are detailed in the User Account Management standard.

9. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Reporting Information Security Incidents standard

Password Safe guideline

Securing Computing and Mobile Storage Devices/Media standard

User Account Management standard

THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U3
Transmission and Sharing of UBC Electronic Information

1. Introduction

1.1 All UBC Electronic Information that is electronically or physically transmitted is at risk of being intercepted and copied by unauthorized parties. Users of UBC Systems have a responsibility to protect this information, according to its classification under the Security Classification of UBC Electronic Information standard.

1.2 This document provides standards on how to transmit or share UBC Electronic Information in a secure manner.

1.3 The Chief information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Key Considerations when Transmitting and Sharing UBC Electronic Information

2.1 Only transmit the minimum amount of information required to complete a task (the Principle of Least Privilege). Do not transmit any information that is not required (e.g. do not include Social Insurance Number and Date of Birth unless necessary). Where possible, do not transmit information that could be used to identify unique individuals.

2.2 Where possible, do not copy, extract or download Medium, High or Very High Risk Information from ERPs.

2.3 Medium, High or Very High Risk Information may be shared with other UBC employees on a 'need to know' basis, when their role at UBC requires them to have access to perform their duties.

2.4 Computing services based outside of Canada (such as Gmail) are not permitted for transmission or sharing of Personal Information unless a Privacy Impact Assessment (PIA) has been conducted for that service, and the risks of storage outside of Canada have been considered and accepted. Please refer to the PIA Process Overview for more information.

2.5 Before Medium, High or Very High Risk Information is shared with Service Providers, Users must ensure the recipient is compliant with all requirements in the Outsourcing and Service Provider Management standard.

3. Acceptable Methods of Transmitting and Sharing UBC Electronic Information

3.1 The table below provides requirements for Users of UBC Systems on how to appropriately transmit or share UBC Electronic Information based upon the Security Classification of UBC Electronic Information standard.

Method of Transmission	Information Security Classification			
	Very High Risk	High Risk	Medium Risk	Low Risk
UBC Email Accounts (e.g. FASmail)	Acceptable only when placed in encrypted email attachments	Acceptable, although if you are sending significant amounts of this information it is best practice to put it in an encrypted attachment		Recommended
Personal Email Accounts (e.g. Gmail, Hotmail)	Not permitted			Not recommended
UBC File Sharing, Collaboration & Messaging Tools[1] (e.g. SharePoint, OneDrive, Teams, Zoom, network shared folders)	Recommended			
Other/Personal File Sharing, Collaboration & Messaging Tools (e.g. Dropbox, Google Drives / Docs / Hangouts, Skype, Slack, Facebook)	Not permitted, unless approved by PIA			Not recommended
Mobile Storage Devices/ Media (e.g. USB drives, CDs/DVDs, tapes)	Encryption is required		Encryption is strongly recommended	Acceptable
Websites Hosted Within Canada	Permitted with authentication and HTTPS (encrypted) connections			HTTPS (encrypted) strongly recommended[2]

[1] Endorsed by the CIO or the Administrative Head of Unit as an acceptable method for transmitting and sharing all UBC Electronic Information.
[2] All Canadian federal government websites were mandated to be HTTPS by September 30, 2019.

Method of Transmission	Information Security Classification			
	Very High Risk	High Risk	Medium Risk	Low Risk
Websites Hosted Outside Canada	Not permitted, unless approved by PIA		Permitted with authentication and HTTPS (encrypted) connections	HTTPS (encrypted) strongly recommended[2]
Other Internet Transmissions (e.g. SSH, FTPS, SFTP)	Permitted with authentication and encrypted connections (insecure internet transmissions e.g. Telnet, FTP are not permitted)			
Fax	Only permitted when sending/receiving fax machines are in secure locations (see Faxing guideline)			

3.2 Section 3.1 does not prevent the use of UBC scanners/copiers on the University network to scan documents and email them to UBC email accounts regardless of the classification of the information in those documents.

3.3 In addition to section 3.1, UBC Systems and services must also comply with the Internet-facing Systems and Services standard.

3.4 Subject to section 3.1, if the User is using personal accounts or other information sharing tools to share UBC Electronic Information, they are responsible for ensuring that a copy of this information is stored on UBC Systems, located in UBC Datacentres or in other authorized locations, in addition to any desktop computers and Mobile Devices, at all times.

3.5 For the purpose of section 3.4, the following are authorized locations:

- 3.5.1 Datacentres at other higher education institutions and health authorities in Canada;
- 3.5.2 EduCloud;
- 3.5.3 Q9 Datacentre (Kamloops);
- 3.5.4 Compute Canada;
- 3.5.5 AWS Canada; and
- 3.5.6 other third party locations approved by the CISO.

3.6 For detailed information about encryption requirements, including how to encrypt documents and Devices, refer to the Encryption Requirements standard.

3.7 For further guidance or assistance with protecting UBC Electronic Information, please contact University IT Support Staff.

4. Email Forwarding from UBC Email Accounts

4.1 Automatically forwarding or redirecting UBC email accounts to non-UBC accounts (“auto-forwarding”) is only acceptable for UBC faculty and staff members who have appointments at other institutions and have difficulty managing multiple work email accounts. Under these circumstances, it is acceptable to auto-forward the UBC email account to the email account at the other institution, provided that:

- 4.1.1 the other institution is a public sector institution located in Canada;
- 4.1.2 the other institution’s email system is at least as secure as UBC’s email system; and
- 4.1.3 the staff or faculty member ensures that copies of emails of business value are returned to UBC Systems, so that they are managed in accordance with UBC’s Records Management Policy.

4.2 Forwarding or redirecting UBC email accounts that are used to transmit UBC Electronic Information to a personal email account is not permitted.

Case Study: Receiving Emails from Students

Students sometimes send emails to their instructors containing personal information about themselves. It is acceptable for instructors to receive and respond to these emails, as long as they only do so using their UBC email accounts. If the student wants to send or receive some extremely sensitive information, such as a medical report, the instructor should encourage the use of encryption on the document to ensure it is secure.

5. Additional Requirements for Merchant Systems

5.1 Due to the sensitivity of Payment Card Industry (PCI) Information, it is subject to the following additional requirements:

5.1.1 PCI Information must only be stored in approved Merchant Systems;

5.1.2 PCI Information must never be transmitted via email or instant messaging systems. This activity is prohibited;

5.1.3 PCI Information must never be transmitted unencrypted by any of the other above methods;

5.1.4 media containing PCI Information must be sent by secured courier or other delivery method that can be accurately tracked; and

5.1.5 management must approve the transfer of PCI Information from a secured area.

6. Receiving Information from Third Parties

6.1 Individuals who are not UBC employees, such as students, sometimes use insecure transmission methods, such as personal email accounts, to transmit their information to UBC. While it is acceptable to receive information in this way, we should encourage these individuals to take measures to minimize the risk of interception by unauthorized parties, such as encrypting files.

7. Related Documents and Resources

Security Classification of UBC Electronic Information standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

BC Freedom of Information and Protection of Privacy Act (FIPPA)

Outsourcing and Service Provider Management standard

Faxing guideline

Internet-facing Systems and Services standard

Encryption Requirements standard

Policy GA4, Records Management

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U4
Reporting Information Security Incidents

1. Introduction

1.1 Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems on campus. Incidents can be accidental or deliberate attempts to break into systems; purpose or consequence can be from benign to malicious. Regardless, each incident requires a careful response, at a level commensurate with its potential to cause harm to an individual and the University, as a whole, as defined in the UBC Incident Response Plan.

1.2 This document defines standards for Users to report any suspicious incidents relating to the security of UBC Electronic Information and Systems. University IT Support Staff (including both departmental IT and UBC IT staff) are responsible for handling security incidents in coordination with UBC Cybersecurity.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Incidents That Must be Reported

2.1 Users must report the following information security incidents (if there is uncertainty whether a violation has occurred, Users must err on the side of caution and report the incident anyway):

2.1.1 all violations of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems; examples include but are not limited to:

2.1.1.1 use of UBC computing facilities to commit illegal acts;

2.1.1.2 unsolicited or spam email originating from UBC sources;

2.1.1.3 unauthorized access, use, alteration or destruction of UBC Electronic Information or UBC Systems, including but not limited to: software, computing equipment, Merchant Systems, network equipment and services;

2.1.1.4 theft of any UBC Electronic Information whether it be via electronic means or physical theft of any Device containing this information; and

2.1.1.5 loss or theft of any Multi-Factor Authentication Device (MFA Device).

2.1.2 unauthorized wireless access points discovered in either merchant areas or areas accessing, transmitting or storing UBC Electronic Information; and

2.1.3 use of Malicious Code, which may show up as unexplained behavior on desktops, laptops or servers such as webpages opening by themselves, new files or folders appearing on the local hard drive, and lockouts of user accounts.

3. How to Report Incidents

3.1 Users must immediately report all suspected information security incidents as follows:

3.1.1 to security@ubc.ca or via phone to the IT Service Centre at 604-822-6141. UBC Cybersecurity will coordinate the incident as required in accordance with the UBC Incident Response Plan;

3.1.2 to their supervisor and University IT Support Staff who are assigned to their unit; and

3.1.3 where the incident involves physical security issues on a UBC campus, in addition to information security issues, to Campus Security.

3.2 It is essential to report incidents immediately, as time is of the essence when dealing with information security breaches and other potentially damaging incidents arising from Malicious Code.

4. Related Documents and Resources

UBC Incident Response Plan

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U5
Encryption Requirements

1. Introduction

1.1 Encryption is the process of making information unreadable to protect it from unauthorized access. After information has been encrypted, a secret key or password is needed to unencrypt it and make it readable again. This document defines standards that Users must comply with for encrypting Devices and files used to access or store UBC Electronic Information so that the information is protected from unauthorized access. This standard may also be used to protect the User's own personal data, e.g. personal banking information.

1.2 This standard incorporates the legal requirement to encrypt Personal Information stored on Devices, which has been affirmed by the British Columbia Information and Privacy Commissioner in their interpretation of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA).

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Password Protection and Zipping

2.1 Password protecting a Device or file merely creates a barrier that can be easily bypassed by a technically knowledgeable individual. By contrast, encrypting a Device or file protects information by "scrambling" it to make it unreadable. It is virtually impossible to bypass encryption that complies with UBC standards.

2.2 Also, zipping files does not automatically encrypt them; a zip file is simply a way to compress data into an easy-to-transport package. Most zip programs contain the ability to protect the compressed file with strong encryption, but this feature is not turned on by default.

3. Device-Level Encryption Requirements

3.1 Encryption requirements apply to Devices, whether UBC-supplied or personally-owned, that are used to access UBC Electronic Information and Systems, or store UBC Electronic Information. Encryption must be implemented as follows:

Device Types	Encryption Requirements	Recommended Toolset
Laptop and desktop computers	Full disk encryption is required. For Users Working Remotely on personally-owned desktop or laptop computers, refer to the Working Remotely standard for supplemental guidance.	Use native encryption for Windows (BitLocker), macOS (FileVault) or Linux (see section 5, Encryption of Devices using Operating Systems other than Microsoft Windows and Apple macOS).
Smartphones, tablets and PDAs	Device-level encryption is required.	iOS and Android Devices with a vendor-supported OS (still receiving updates) connecting to FASmail using the native ActiveSync client are automatically encrypted.
Mobile Storage Devices/Media	Device/media-level encryption is required.	Refer to How to Encrypt USB Sticks and Other Removable Media guideline.

Servers		
Servers located in datacentres that comply with the Physical Security of UBC Datacentres standard	No full disk encryption required.	n/a
Third party servers that have an equivalent level of security to the Physical Security of UBC Datacentres including: • Datacentres at other higher education institutions and health authorities, in Canada • EduCloud • Compute Canada HPC • Other third party servers approved by the CISO	No full disk encryption required.	n/a
Other servers than listed above.	Full disk encryption is required. See section 4 for Cloud-based Encryption Requirements, e.g. AWS Canada and SaaS.	Use native encryption for Windows (BitLocker) or Linux (see section 5).

3.2 Even in situations where encryption is not required in section 3.1, encryption may nevertheless be required to meet additional obligations such as contractual requirements.

3.3 Using Mobile Devices to store High or Very High Risk Information is not recommended. However, there may be situations where this is necessary. For example, USB sticks are commonly used to transport large amounts of information. Also, if a Mobile Device is used to access email, these emails (including emails containing High or Very High Risk Information) may be backed up automatically on the Device. In both of these situations, encryption would be required.

3.4 If Users are travelling abroad with a laptop that has an encrypted drive or that contains encrypted information, authorities of that country may require them to unencrypt the information or hand over the encryption keys (see Security Considerations for International Travel with Mobile Devices guideline).

3.5 If a Device is lost or stolen, it is essential for the University to be able to accurately report on its encryption status. Users must provide a written confirmation of the encryption status and method (e.g. encrypted with BitLocker) at the time of loss or theft. University IT Support Staff may be able to assist in providing this information.

4. Cloud-based Encryption Requirements

4.1 Encryption requirements apply to UBC Electronic Information and Systems stored and accessed in cloud-based technologies. Encryption must be implemented as follows:

Service Types	Encryption Requirements	Recommended Toolset
Virtual servers, e.g. AWS Canada and Compute Canada Cloud (IaaS). Object-based storage, e.g. AWS S3 bucket.	Full volume encryption is required.	Use native encryption for Windows (BitLocker), Linux (see section 5) or service.

Service Types	Encryption Requirements	Recommended Toolset
Software as a Service (SaaS), e.g. Workday Platform as a Service (PaaS), e.g. platform.sh	High or Very High Risk Information must be encrypted. Low and Medium Risk Information should be encrypted where possible.	n/a

4.2 To limit vendor access to UBC Electronic Information, encryption keys should be stored with UBC (and not the vendor) unless not technically feasible.

5. Encryption of Devices using Operating Systems other than Microsoft Windows and Apple macOS (e.g. Linux)

5.1 Due to operability or performance constraints, full disk encryption is not always viable for already deployed Operating Systems other than Microsoft Windows and Apple macOS (e.g. Linux). If full disk encryption isn't viable then any of the following alternative options are considered acceptable:

5.1.1 an encrypted Virtual Machine (VM);

5.1.2 an encrypted partition;

5.1.3 an encrypted home directory; or

5.1.4 a securely mounted directory in the UDC, e.g. TeamShare or Home Drive.

5.2 The local IT team(s) must advise Users who implement any of the above options that:

5.2.1 these alternative options are not as secure as full disk encryption;

5.2.2 the User must store all Medium, High or Very High Risk Information in one of the options listed in Section 5.1; and

5.2.3 the User must put full disk encryption in place as soon as practically possible.

5.3 University IT Support Staff must also send an email to information.security@ubc.ca identifying any Users who have implemented any alternatives to full disk encryption. The CISO will maintain a record of these Users and on a periodic schedule review viability to transition to full disk encryption.

6. Encryption Exemptions

6.1 The following types of UBC Systems are exempt from encryption requirements if they are fully compliant with the Encryption Exemption Criteria and they have been documented in a completed and submitted Encryption Exemption Attestation Form:

6.1.1 Direct Attached Storage (DAS);

6.1.2 kiosks;

6.1.3 public workstations;

6.1.4 instructional lab workstations;

6.1.5 instrument controllers; and

6.1.6 lectern/podium workstations.

6.2 If the UBC System cannot be encrypted and is not compliant with the Encryption Exemption Criteria, then a variance must be requested from the CIO, as per the Requesting Variances from Information Security Standards standard.

7. File-Level Encryption Requirements

7.1 For instructions on encrypting Word, Excel and other general files, refer to the How to Encrypt Files Using Common Applications guideline.

7.2 For requirements on emailing UBC Electronic Information, refer to the Transmission and Sharing of UBC Electronic Information standard.

8. Password Requirements

8.1 Strong passphrases or passwords must be used for encryption in compliance with the Passphrase and Password Protection standard.

8.2 If the password (also called a "key") is forgotten or lost, the data may be unrecoverable. Therefore, it is essential to have a key recovery strategy. Where operationally feasible, faculty and staff can use the University's Key Escrow services, or simply write down the password and store it in a secure location such as a safe. Further information about key recovery can be found in the Cryptographic Controls standard.

9. Technical Requirements

9.1 UBC's minimum encryption standard is AES-128 bit encryption or equivalent; AES-256 bit encryption is recommended. Further technical requirements can be found in the Cryptographic Controls standard. University IT Support Staff, including staff in the IT Service Centre, are available to assist Users to implement these requirements where necessary.

10. Related Documents and Resources

BC Freedom of Information and Protection of Privacy Act (FIPPA)

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Working Remotely standard

Setting Up UBC Faculty & Staff Email Using ActiveSync

How to Encrypt USB Sticks and Other Removable Media guideline

Physical Security of UBC Datacentres standard

Security Considerations for International Travel with Mobile Devices guideline

Encryption Exemption Criteria

Encryption Exemption Attestation Form (with CWL credentials)

Systems for Encryption Exemption

Requesting Variances from Information Security Standards standard

How to Encrypt Files Using Common Applications guideline

Transmission and Sharing of UBC Electronic Information standard

Passphrase and Password Protection standard

Cryptographic Controls standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U6
Working Remotely

1. Introduction

1.1 During the course of their employment, many UBC employees need to work remotely (including outside of Canada) with UBC Electronic Information, such as research, financial and Personal Information. UBC Electronic Information is generally more at risk of being compromised, corrupted or lost when accessed remotely than when accessed from internal systems, due to:

1.1.1 the vulnerability of laptops or other Mobile Devices to theft or loss;

1.1.2 the risk of unauthorized persons (e.g. family members, commercial service providers) viewing information;

1.1.3 lower standards of physical and electronic security than on UBC premises; and

1.1.4 retention of information on mobile or remote systems without some Users being aware (e.g. cached webpages and email attachments).

1.2 This standard defines requirements for UBC employees working remotely with UBC Electronic Information on all Devices. Working remotely includes but is not limited to:

1.2.1 working from home;

1.2.2 travelling;

1.2.3 working from a coffee shop or conference;

1.2.4 working from a location using the Eduroam wireless network; and

1.2.5 working within a health authority facility where the network is not under the control of UBC.

1.3 This standard must be read in conjunction with the Encryption Requirements and Securing Computing and Data Storage Devices/Media standards. These standards apply to all Devices used for University Business—no matter whether they are owned by the University, by the User, or by a third party.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Secure Access Methods

2.1 Wherever possible, UBC Electronic Information should be remotely accessed through a UBC System, rather than downloaded onto a Device, as this will significantly reduce the risk of loss or theft. The following are the preferred secure methods for Remote Access:

2.1.1 The recommended methods to access information are to use a Virtual Private Network (VPN) or SSH (secure shell) interface.

2.1.2 When connecting via VPN, use remote desktop (RDP) where possible, as this presents the lowest risk for Remote Access by keeping data at the university. Important points to note:

2.1.2.1 RDP must not be used without a VPN connection;

2.1.2.2 don't map remote drives to your local Workstation; and

2.1.2.3 for information on using RDP, contact your University IT Support Staff.

2.1.3 Alternatively, a Virtual Desktop Interface (VDI) can be used, only accessing the information inside the VDI session. VDI is a service available through UBC IT, which creates a "virtual" computer that can be accessed from home computers, laptops, desktops, tablets and even smartphones.

2.1.4 Microsoft Remote Desktop Services (RDS, previously Terminal Services) is also an acceptable secure access method.

2.1.5 For access methods other than the above, confirm with University IT Support Staff that the method and configuration are secure.

2.2 Remote Access must be in compliance with the Network Protocol Requirements section of the Internet-facing Systems and Services standard.

2.3 Do not use a network connection if a 'certificate error' window or other alert appears when trying to connect to a UBC System via a secure access method (as outlined in section 2.1), or if the User is otherwise uncertain about the safety of the network.

3. Supplemental Guidance for Personally-owned Equipment

3.1 If a personally-owned desktop or laptop computer is accessing UBC Electronic Information and Systems using VPN with RDP, VDI or RDS then device-level encryption is not required, but is recommended.

3.2 Ensure personally-owned routers and home networks (including IoT Devices) are properly secured (see Securing your Home Router guideline).

4. Physical Security

4.1 Reasonable measures must be taken to prevent or reduce the possibility of loss or theft of Devices (including Multi-Factor Authentication Devices) that are used to access or protect UBC Electronic Information such as:

4.1.1 being aware of others looking over one's shoulder at the Device when working in public locations such as coffee shops, aircraft and other public transport;

4.1.2 not leaving Devices unattended in a public place, especially well-travelled areas such as airport lounges and coffee shops; and

4.1.3 keeping Devices secured when working from home, e.g. storing them in a physically secured area and ensuring UBC Electronic Information cannot be accessed by family members.

4.2 Reasonable measures must be taken to prevent or reduce the possibility of loss or theft of Multi-Factor Authentication Devices.

5. Third Party Devices and Networks

5.1 Do not access Medium, High or Very High Risk Information using third party Devices, such as kiosks in public libraries, hotels, airports, and cyber cafes, unless the Device is owned by another higher education institution or health authority in partnership with UBC (e.g. a collaborator).

5.2 When accessing public Wi-Fi networks, such as those in airports and coffee shops, do not use the connection if a 'certificate error' window or other alert appears when trying to connect to a UBC System via a secure access method (as outlined in section 2), or if the User is otherwise uncertain about the safety of the network.

6. Related Documents and Resources

Encryption Requirements standard

Securing Computing and Mobile Storage Devices/Media standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

UBC IT myVPN Service

Remote Desktop Protocol (RDP)

UBC IT Virtual Desktop Interface (VDI)

Internet-facing Systems and Services standard

Securing your Home Router guideline

UBC IT Guide to Working off Campus

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U7
Securing Computing and Mobile Storage Devices/Media

1. Introduction

1.1 All Devices used for University Business—no matter whether they are owned by the University, by the User, or by a third party—need to be protected from theft and/or unauthorized access. This standard specifies the minimum security requirements that Users must comply with to protect these Devices. University IT Support Staff, including staff in the IT Service Centre, are available to assist Users in implementing these requirements where necessary.

1.2 Two broad categories of Devices are covered by this standard:

1.2.1 Computing Devices, e.g. Servers, desktop and laptop computers, tablets and smartphones; and

1.2.2 Mobile Storage Devices/Media, e.g. external hard drives, DVDs, and USB sticks.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Electronic Security

2.1 Computing Devices used for University Business must comply with the following electronic security requirements. Users with IT-related responsibilities should also see the Vulnerability Management standard.

	Servers	Workstations	Smartphones & Tablets
Password Control	All Devices must be password-protected in accordance with the Passphrase and Password Protection standard. Always lock Devices or log out before leaving them unattended.		
Screensaver Locks/Idle Timeout	Console automatically locks after no more than 5 minutes of inactivity.	User interface automatically locks after no more than 30 minutes of inactivity (5 minutes is recommended for Devices storing Medium, High or Very High Risk Information).	
Device Location	n/a		Enable any features that will allow the Device to be remotely located in the event of loss or theft.
Data Destruction	n/a		Enable the feature that automatically erases data if 10 consecutive incorrect passwords are entered.
Remote Wiping	n/a		Enable any features that will allow data stored on the Device to be erased in the event of loss or theft.
Endpoint Detection and Response (EDR)	EDR software approved by the CISO must be installed on all UBC-owned Servers.	EDR software approved by the CISO must be installed on all UBC-owned Workstations, where technically possible.	n/a

Malware and Spyware Protection	On Computing Devices not required to have EDR, install up-to-date anti-malware and spyware cleaning software (except for smartphones and tablets that do not offer this feature) and configure it to update at least once per day. See the UBC IT Malware Protection page.	
Automatic Blocking of Malicious Websites	Servers on-premises and in the cloud (Infrastructure as a Service) must be protected by a DNS firewall. It is recommended that Servers on-premises use UBC Domain Name Servers, which make use of DNS firewall protection.	UBC-owned Devices that access, process or store Medium, High or Very High Risk Information must be protected by a DNS firewall. It is recommended that on-premises Devices use UBC Domain Name Servers, which make use of DNS firewall protection. For all other Devices, a DNS firewall is recommended.
Firewalls	Install and configure firewalls (except for tablets and smartphones that do not offer this feature). See the Firewalls guideline.	
Operating System	The Device must run a version of its operating system for which security updates continue to be produced and are available. If this is not possible, see the Vulnerability Management standard for compensating controls. If the Device is University-owned, software updates must not be impeded, and no unauthorized changes may be made to the Device.	
		Workstations must be regularly restarted to facilitate patching of vulnerabilities. The recommended frequency for restarting is at least once per week.
Data Availability	Any UBC Electronic Information stored on the Device must be regularly backed up to a secure location and checked periodically (preferably quarterly) to ensure the integrity and availability of the information such that it can be restored. See the Backup guideline.	
Encryption	Refer to the Encryption Requirements standard.	

2.2 Mobile Storage Devices/Media must be encrypted as explained in the Encryption Requirements standard.

3. Physical Security

3.1 For their protection, unattended Devices must be located in one or more of the following areas:

3.1.1 a room or other enclosed area that is locked or otherwise access-controlled; and/or

3.1.2 a locked cabinet or other fixed container such as a locked server cabinet/cage.

3.2 Servers containing significant quantities of High or Very High Risk Information must be hosted in UBC Datacentres that are compliant with the Physical Security of UBC Datacentres standard, or third party datacentres that have an equivalent level of security. To get access to server space in a UBC Datacentre, Users can rent space or use the EduCloud Server Service.

3.3 Keys or swipe cards giving access to Devices must be limited to authorized individuals.

3.4 Measures should be taken to ensure Devices cannot be viewed from outside the secure area, e.g. by drawing curtains or blinds.

3.5 Cable locks are recommended as a supplementary security measure for Computing Devices, but they do not provide sufficient protection by themselves. It is safer to lock portable Devices, such as laptops, in a cabinet out of sight rather than relying on a cable lock.

3.6 The use of alarms is highly recommended, especially to protect Devices used to store Medium, High or Very High Risk Information.

4. Use of Non-University-Owned Devices

4.1 UBC recognizes that it is often convenient for Users to use their personally-owned Devices for work purposes and such use is permitted provided that they manage their Devices in accordance with this standard.

4.2 Some Users may also use Devices supplied by third parties in connection with University Business. Users, in consultation with University IT Support Staff, are responsible for determining whether these Devices meet the minimum security requirements in this standard; for example, Health Authorities have good information security measures in place, and it is acceptable to use their computers for University Business.

5. Special Requirements for Servers

5.1 Servers (especially Web and FTP servers) are attacked on a continual basis. To avoid creating security weaknesses, servers must not be used for general web browsing or email.

5.2 Users must not run server applications on desktops or laptops (e.g. web or FTP servers) that are Internet-facing. Exceptions may be approved by the Administrative Head of Unit, in consultation with University IT Support Staff, provided that compensating controls are put in place to control security risks.

6. Inventory of UBC-owned Laptops and Desktops

6.1 Central UBC IT support staff must maintain an inventory of UBC-owned laptops and desktops that they have deployed, including which Users these Devices are assigned to. All other University IT Support staff are recommended to maintain such inventories.

7. Return of Devices and Information upon Termination

7.1 Upon termination of their employment, Users must return all of the UBC-owned Devices in their possession to an authorized employee of UBC, and must return and delete any UBC Electronic Information stored on their personally-owned Devices.

8. Loss Reporting Requirement

8.1 Users who lose a Device used for University Business (no matter who owns the Device) or suspect that there could have been an unauthorized disclosure of UBC Electronic Information must report the loss/disclosure in accordance with the Reporting Information Security Incidents standard.

9. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Vulnerability Management standard
Passphrase and Password Protection standard
UBC IT Malware Protection
UBC Domain Name Servers
Firewalls guideline
Backup guideline
Encryption Requirements standard
Physical Security of UBC Datacentres standard
Data Centre Co-Location Service
EduCloud Server Service
Reporting Information Security Incidents standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U8
Destruction of UBC Electronic Information

1. Introduction

1.1 A large proportion of UBC Electronic Information is Medium, High or Very High Risk Information, such as student records, personnel records, financial data, and protected health or research information. If this information is not properly removed when no longer required and before the equipment is disposed of, unauthorized access may occur resulting in harm to an individual and/or the University.

1.2 This document defines standards for Users, including Information Stewards/Owners on the destruction and/or sanitization of UBC Electronic Information (data destruction).

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Responsibilities of Users

2.1 Users should only retain information as long as needed or required by policy, legislation or agreement.

2.2 Users are responsible for ensuring that UBC Electronic Information is always removed from a Device before it is transferred to another individual, sold, discarded or taken with the User (with authorization from the Administrative Head of Unit) upon leaving the University. The information needs to be removed even if it does not appear to be Medium, High or Very High Risk. Users should contact University IT Support Staff or the IT Service Centre if they require data destruction assistance.

3. Responsibilities of Service Providers

3.1 Where a third party Service Provider has received copies of UBC Electronic Information for the purpose of UBC work, the Service Provider must destroy all of the information in its possession within seven days of the completion of the project or termination of the agreement, whichever first occurs. Destruction methods must be compliant with this standard and the Administrative Head of Unit must obtain signed confirmation of destruction in a format consistent with the Data Destruction Confirmation procedure.

3.2 Where data destruction is not feasible, Administrative Head of Unit may consult with UBC Cybersecurity to determine appropriate alternate controls.

3.3 This does not apply to collaborations with other research institutions for research purposes where a data retention agreement is in place.

4. Acceptable Data Destruction Methods

4.1 Any of the following are acceptable methods of data destruction:

4.1.1 using a software utility that erases by overwriting or encrypting the data;

4.1.2 magnetically erasing (degaussing) the data;

4.1.3 formatting a Device after encrypting it in compliance with the Encryption Requirements standard; or

4.1.4 using a machine that physically deforms or destroys the Device to prevent the data from being recovered.

4.2 Using the “Empty Recycle Bin/Trash”, “Delete”, “Remove”, and “Format” operating system commands do **not** destroy data and therefore are **not** acceptable methods for preparing media for transfer or disposal.

4.3 Data destruction methods must comply with the minimum standards set out in the IT Media Sanitization (ITSP.40.006) publication issued by the Government of Canada.

5. Special Cases

5.1 To destroy data on flash memory devices (e.g. SD memory cards, USB drives) containing UBC Electronic Information, the User can encrypt the whole device according to the Encryption Requirements standard. After encryption, the User can format the device and reuse it safely.

5.2 Data destruction on smartphones can be accomplished via a factory reset; note that some smartphones have removable memory cards that need to be treated the same as flash memory devices and securely sanitized separate from a phone factory reset. Users can contact their cellular service provider if they are uncertain of how to perform a factory reset.

5.3 Data destruction on IoT Devices can be accomplished via a factory reset; note that some IoT Devices have removable memory cards that need to be treated the same as flash memory devices and securely sanitized separate from a factory reset. Users can contact the device manufacturer if they are uncertain of how to perform a factory reset. Consideration must be given as to whether or not data stored off the device will still be required in the IoT ecosystem, e.g. with service providers. If the data is not required, it must also be destroyed.

5.4 Other imaging devices with a hard drive (e.g. photocopiers, printers, fax machines, etc.) are also subject to the data destruction requirements; additionally, where possible, these devices should have image overwriting enabled. This is a function where scanned or electronic images of a document are immediately overwritten using a data destruction technique. This function is known by various names, e.g. “Immediate Image Overwrite” (Xerox), “Hard Disk Drive Erase Feature” (Canon), “Hard Disk Overwrite Feature” (HP).

6. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Data Destruction Confirmation form

Encryption Requirements standard

IT Media Sanitization (ITSP.40.006)

THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U9
Outsourcing and Service Provider Management

1. Introduction

Service Providers (vendors, contractors, consultants and other non-UBC employees who provide services to UBC) may access, process, store or transmit UBC Electronic Information and Systems in order to deliver agreed-upon services. The increased security risk when access is extended outside of the organization needs to be managed appropriately. This standard is not intended to cover collaborations with other research institutions for research purposes.

This standard explains the information security requirements applicable to all Service Providers. The Administrative Head of Unit who engages a Service Provider is responsible for ensuring compliance with all of these requirements.

1.1 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Security and Privacy Risk Assessment

2.1 Before Service Providers provision software applications or are granted access to UBC Electronic Information and Systems, information security risks must be assessed and managed using the Service Provider Security Checklist.

2.2 In addition to the requirement to use the above checklist, a Privacy Impact Assessment (PIA) is required if Personal Information is involved. Please refer to the PIA Process Overview for more information.

3. Cloud Service Providers

3.1 Cloud services providers (e.g. AWS, Azure) raise significant privacy and information security concerns as they store data outside of the custody of the University. Therefore it is essential to complete a PIA in each situation where these providers will be used.

4. Compliance with Policies and Standards

4.1 Before access is granted to UBC Electronic Information and Systems, the Service Provider must be made aware that it will be subject to Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems, and its accompanying standards.

5. Contractual Requirements

5.1 Service Providers must sign a Security and Confidentiality Agreement (SACA) prior to being granted access to Medium, High or Very High Risk Information. The Administrative Head of Unit may request the Office of the University Counsel to grant a waiver of the requirement for a SACA where the primary contract with the Service Provider contains equivalent privacy and security language. Doctors, lawyers, accountants, auditors, psychologists and other professionals who are bound by a duty of confidentiality do not need to sign a SACA.

6. Storage and Transmission of Information

6.1 Service Providers must store UBC Electronic Information in a logically separated environment, ensuring that the information is not mixed with information belonging to or accessed by other

parties. If this is not possible, Service Providers may use alternative controls, with the written approval of the Administrative Head of Unit, to ensure that the data is secure and can be destroyed after the project is completed.

6.2 Service Providers must ensure that they transmit UBC Electronic Information in accordance with the Transmission and Sharing of UBC Electronic Information standard.

7. Access Controls

7.1 All Service Provider access to UBC Electronic Information and Systems must be granted as follows:

7.1.1 access must be authenticated and role based;

7.1.2 access must be granted on a Principle of Least Privilege (only the minimum level of access that is required to perform their duties); and

7.1.3 wherever possible, access to UBC Systems containing High or Very High Risk Information should be logged.

8. Ongoing Monitoring

8.1 The work of Service Providers must be monitored and reviewed to ensure that privacy, confidentiality and information security requirements are being satisfied.

9. End of Services and Data Destruction

9.1 Immediately upon completion of the project or termination of the agreement, whichever first occurs, the following must take place:

9.1.1 the Administrative Head of Unit must ensure that the Service Provider's access to UBC Electronic Information and Systems is revoked; and

9.1.2 the Service Provider must stop accessing UBC Electronic Information and Systems.

9.2 Within seven days of the completion of the project or termination of the agreement, whichever first occurs, the following must take place:

9.2.1 the Service Provider must return all UBC assets (including access control cards and keys), equipment, and UBC Electronic Information in their possession; and

9.2.2 the Service Provider must destroy all UBC Electronic Information and hard copies of this information in its possession in compliance with the Destruction of UBC Electronic Information standard.

10. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Service Provider Security Checklist

Privacy Impact Assessment (PIA)

Security and Confidentiality Agreement

BC Freedom of Information and Protection of Privacy Act (FIPPA)

Transmission and Sharing of Electronic Information standard

Destruction of UBC Electronic Information standard

THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U10
Accessing Electronic Accounts of Other Users

1. Introduction

1.1 This document defines standards that Users (typically supervisors and investigators) must comply with to gain access to electronic accounts of other Users on UBC Systems, such as UBC email accounts, UBC file sharing, collaboration and messaging accounts, Home Drive, voicemail accounts, internet usage records and telephone logs.

1.2 This standard does not apply to electronic accounts that are not owned by individual Users, such as building access logs or shared email accounts.

1.3 This standard does not apply to system administrators or other technical personnel who, in the course of carrying out their duties, require access for technical purposes, such as installation, maintenance, repair, troubleshooting or upgrading.

1.4 The purpose of this standard is to protect the Personal Information of individual account holders while continuing to allow access to information required for University purposes.

1.5 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Access with Consent

2.1 Policy SC14 authorizes reasonable personal use of UBC Systems. For privacy reasons, it is preferable to get the consent of Users before accessing electronic accounts and records.

Consent must be in writing, but does not need to be signed (an email is acceptable). The following language is recommended for a consent statement:

> I, [NAME], authorize UBC to access [ACCOUNTS/RECORDS] for the following purpose: [PURPOSE]. This authorization is effective until [DATE].

2.2 If the consent of the User has been secured, authorization of the Administrative Head of Unit or the Office of the University Counsel is not required to access the account or records in question.

3. Access without Consent

3.1 It is occasionally necessary to gain access to an electronic account or record without the User's consent. To ensure that the University's Business requirements are balanced against the User's privacy interests, access without consent requires the authorization of the Administrative Head of Unit and the Office of the University Counsel. This authorization will depend on the type of information intended to be accessed and how the information will be used after it has been accessed.

4. Criteria for Access to UBC Electronic Information without Consent

4.1 If UBC Electronic Information only needs to be viewed, then the Administrative Head of Unit and the Office of the University Counsel will authorize access the electronic accounts/records provided that the University is legally required to do so, or:

4.1.1 there is a pressing reason to view this information for University Business purposes; and

4.1.2 consent of the User cannot be secured despite making reasonable attempts to do so, e.g. the User is incapacitated, has gone on vacation without leaving contact information, or has been terminated and is unwilling or unavailable to provide consent.

4.2 When accessing accounts or records to view UBC Electronic Information, reasonable efforts must be made to avoid viewing the User's Personal Use Records. If Personal Use Records have been inadvertently viewed, then these records must not be copied, altered, deleted, used or disclosed unless

they provide evidence of a violation of law, in which case the matter must be referred to the Office of the University Counsel, which will determine the appropriate action.

4.3 In addition to Personal Use Records, accounts may also contain other sensitive information, such as teaching materials or research information. The confidentiality of this information must be respected as its unauthorized use and disclosure may harm the interests of the User and the University as a whole.

Examples Of User Accounts

An employee has been incapacitated in a motor vehicle accident. Her supervisor needs to access the employee's work email account to check for any time-sensitive work-related messages, but the employee is unable to consent to this access. Under these circumstances, access would normally be authorized. However, the supervisor should not read the employee's personal messages.

5. Criteria for Access to Personal Use Records without Consent

5.1 If Personal Use Records need to be viewed, then the Administrative Head of Unit and the Office of the University Counsel will only authorize access to electronic accounts/records if the University is legally required to do so, or if securing consent would compromise:

5.1.1 the health or safety of an individual or a group of people,

5.1.2 the availability or accuracy of the information; or

5.1.3 an investigation or a proceeding related to a breach of law or policy or the employment of the User.

6. Procedure for Access

6.1 To access accounts and records, the Request to Access Electronic Accounts of Other Users form must be completed and submitted to the administrator who controls access to the account. If the User's consent is not obtained, the Administrative Head of Unit and the Office of the University Counsel must be requested to sign the access form to authorize access. The administrator will grant access to the account/records only for the period of time specified in the access form.

7. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Request to Access Electronic Accounts of Other Users form

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U11
Securing Internet of Things (IoT) Devices

1. Introduction

1.1 Internet of Things (IoT) Devices pose special risks and must be assessed to ensure that they do not put UBC Electronic Information and Systems at risk.

1.2 This standard defines the minimum security requirements that Users must comply with to protect these Devices throughout their lifecycle. University IT Support Staff, including staff in the IT Service Centre, are available to assist Users in implementing these requirements where necessary.

1.3 All IoT Devices used for University Business—no matter whether they are owned by the University, by the User, or by a third party—need to be protected from theft of the device and/or unauthorized access to UBC Electronic Information and Systems.

1.4 This standard is meant to cover only IoT Devices, including but not limited to:

1.4.1 Devices used for remote automation and/or monitoring (e.g. controllers, sensors, HVAC systems);

1.4.2 network-connected imaging Devices (e.g. scanners, printers, webcams, multi-function devices);

1.4.3 Devices with network-connected controllers (e.g. medical devices, scientific instruments, industrial control systems, PLCs);

1.4.4 “Smart” Devices or appliances (e.g. speakers, TVs, lightbulbs, refrigerators, doorbells, IoT bridges and hubs);

1.4.5 single board computers (SBCs) (e.g. Raspberry Pis, Arduinos, Tinkerboards), when not configured as Mobile Devices, Servers or Workstations; and

1.4.6 if there is any doubt about whether or not a Device is covered, consult the CISO.

1.5 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. IoT Device Risk

2.1 Users must take a risk-based approach to securing IoT Devices based on the UBC Electronic Information that the Device stores or has access to. Consideration must be given to:

2.1.1 what information can be collected, accessed or stored, e.g. what can be listened to, seen or captured through audio or imaging;

2.1.2 what other Devices (including sensors) the IoT Device is connected to;

2.1.3 what Devices or systems can be controlled, e.g. temperature of a research sample fridge or control of a power system;

2.1.4 where the IoT Device is physically located; and

2.1.5 whether the Device is integral to University Business.

2.2 Users must minimize the risk to UBC as much as possible by capturing the least amount of data required for the operation of the IoT Device. For example:

2.2.1 reduce camera field of view to only capture the minimum required area, or disable camera when not required;

2.2.2 ensure IoT Devices that capture audio are located or configured such that they won’t capture unintended audio or conversations (including voice recognition commands that could be issued by unauthorized personnel); and

2.2.3 disable or remove any sensors that are not required.

2.3 IoT Devices that capture video images must also be in compliance with Policy SC16, Safety and Security Cameras.

2.4 When deploying IoT Devices, the security classification of information collected and transmitted must be identified. The Device must be assessed to determine if any UBC Electronic Information is being transmitted, and to what location(s).

2.4.1 Projects or initiatives involving IoT Devices that collect, store or access Personal Information must undergo a Privacy Impact Assessment (PIA), as set out in the Privacy Impact Assessment requirements.

2.4.2 IoT Devices that store Medium, High or Very High Risk Information on third party systems must have a copy of this information stored on UBC Systems at all times.

3. Physical Security

3.1 Based on IoT Device risk, the following physical security measures should be taken to protect IoT Devices against theft, alteration or misuse. Consideration should be given to removable components of IoT Devices, e.g. memory cards, batteries.

3.1.1 Where possible, unattended IoT Devices must be located in a room or other enclosed space (e.g. cabinet or other fixed container such as a server cabinet/cage) that is alarmed, locked and/or otherwise accessed-controlled.

3.1.2 Keys or swipe cards giving access to IoT Devices must be limited to authorized individuals.

3.2 To prevent unauthorized access, all physical interfaces to IoT Devices (e.g. USB, serial or Ethernet ports) must be secured against unauthorized physical access.

4. Electronic Security

4.1 All interfaces (e.g. mobile applications, web applications, APIs) to IoT Devices must be configured based on the Principle of Least Privilege and secured where necessary.

4.2 All control interfaces used to configure IoT Devices must be secured against unauthorized access and changes.

4.3 Passwords and passphrases used with IoT Devices must be in compliance with UBC's Passphrase and Password Protection standard (e.g. not weak, re-used, pre-defined or hardcoded). These include passwords and accounts used for third party vendor accounts (e.g. Facebook, Google, Apple), and for IoT Device firmware and applications used to manage them.

4.3.1 Where a hard-coded password exists, the risk must be mitigated with compensating controls approved by the CISO.

4.4 To facilitate restoration of services dependent upon IoT Devices, a backup of the configuration of IoT Devices should be maintained in a secure location. Examples of backups include screenshots or exports of configuration details, or configuration scripts.

4.5 IoT Devices that store Medium, High or Very High Risk Information must be regularly backed up to a secure location and checked periodically (preferably quarterly) to ensure the integrity and availability of the information such that it can be restored. See the Backup guideline.

4.6 Where possible, enable features that will allow the IoT Device, including data and configuration, to be remotely erased in the event of loss or theft.

5. Network Security

5.1 All network traffic to or from IoT Devices must be secured against unauthorized access, in compliance with the Transmission and Sharing of UBC Electronic Information standard.

5.2 Interference with other University wireless networks must be managed in compliance with Policy SC11, Management of the Wireless Network. Wireless Access Points (including extenders/repeaters) used to facilitate connectivity for IoT Devices must also be in compliance with Policy SC11.

5.3 If the only traffic an IoT Device delivers over TCP/IP networks is publicly-accessible or Low Risk Information then the IoT Device must be secured in compliance with the Internet-facing Systems and

Services standard. This includes IoT bridges and hubs, such as Zigbee, Z-Wave, Bluetooth and other non-TCP/IP devices that are connected to TCP/IP networks.

5.4 All other TCP/IP network-connected IoT Devices (including IoT bridges and hubs) must only be internet accessible via a Virtual Private Network (VPN) unless an exception has been approved by the CISO.

6. Hardening Requirements

6.1 To prevent unauthorized access, pairings or connections, IoT Devices must not be left in set-up, reset or pairing mode.

6.2 Unless required for the function of the Device, IoT Devices must not be left in Bluetooth Discovery Mode.

6.3 Prior to being deployed in production, default settings of IoT Devices must be reviewed to ensure insecure configurations have been remediated.

6.4 Unneeded or insecure network services running on IoT Devices must be disabled.

6.5 Unneeded physical and wireless interfaces on IoT Devices must be disabled where possible.

6.6 IoT Devices must not use weak or unencrypted protocols for data transmission anywhere within the ecosystem, including at rest, in transit, or during processing.

6.7 Operating system, firmware and software on IoT Devices must be updated to address IT vulnerabilities in compliance with the Vulnerability Management standard. Following every update, the implications of changes must be assessed to ensure the device is still secure.

6.8 Operating system, firmware and software updates to IoT Devices must be controlled so that all updates are automated where possible, or only delivered by authorized personnel. Updates should be made in a secure manner, using secure mechanisms where possible. Examples of secure mechanisms are:

6.8.1 update is signed and signature-verified;

6.8.2 update is delivered to the Device through an encrypted communication channel;

6.8.3 update is manually transferred to the Device by an authenticated administrator only; and

6.8.4 update is received only from a vendor-authorized site.

6.9 Deprecated or unsupported hardware must be replaced, or compensating controls approved by the CISO must be implemented.

6.10 UBC Electronic Information on IoT Devices must be destroyed and/or sanitized before the device is decommissioned, in compliance with the Destruction of UBC Electronic Information standard.

6.11 Any customization of the operating system or firmware of an IoT Device not performed by the manufacturer must be in compliance with the Development and Modification of Software Applications standard.

7. Requirements for Merchant Systems

7.1 Point of Interaction (POI), e.g. PIN pad, Unattended Cardholder-Activated Terminal (UCAT), and other IoT Devices must not be used in Merchant Systems without authorization from the UBC PCI Compliance Working Group.

8. Logging and Monitoring Requirements

8.1 IoT Device logs should be captured and monitored in compliance with the Logging and Monitoring of UBC Systems standard where possible.

8.2 Based on section 2, IoT Device Risk, IoT Devices must be:

8.2.1 monitored for availability and checked for unusual behavior or performance to ensure a timely and appropriate response; and

8.2.2 recorded in an inventory, maintained by the User and provided to University IT Support Staff prior to going into production. Refer to the sample inventory attached to this standard. At a minimum, the inventory should contain the Device make, model, serial number (or other method of unique

identification), description, associated service(s), location, technical contact and security classification of information collected. Where applicable, include the following:

8.2.2.1 radio frequency bands in use, e.g. 900 MHz, 2.4 GHz, 5.4 GHz; and

8.2.2.2 active over-the-air modes and protocols, e.g. LoRa, Z-Wave, Zigbee, Thread.

9. Loss Reporting Requirement

9.1 Users who lose an IoT Device used for University Business (no matter who owns the IoT Device) or suspect that there could have been an unauthorized disclosure of UBC Electronic Information must report the loss/disclosure in accordance with the Reporting Information Security Incidents standard.

10. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Policy SC16, Safety and Security Cameras

Privacy Impact Assessment (PIA)

Passphrase and Password Protection standard

Backup guideline

Transmission and Sharing of UBC Electronic Information standard

Policy SC11, Management of the Wireless Network

Internet-facing Systems and Services standard

Vulnerability Management standard

Destruction of UBC Electronic Information

Development and Modification of Software Applications standard

Logging and Monitoring of UBC Systems standard

Sample Inventory

Reporting Information Security Incidents standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M1
Requesting Variances from Information Security Standards

1. Introduction

1.1 In order to protect University information assets, the Chief Information Officer (CIO) has issued binding Information Security Standards. Academic and administrative units that wish to deviate from these Information Security Standards are required to request a variance from the CIO.

1.2 This standard establishes the procedure for Administrative Heads of Unit to request such a variance.

1.3 The CIO has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Variance Request Procedure

2.1 Initial Request - the Administrative Head of Unit must submit the following information to information.security@ubc.ca:

2.1.1 contact information;

2.1.2 description of the requested variance and expected duration;

2.1.3 explanation of why the variance is warranted;

2.1.4 analysis of risk associated with granting the variance, and what controls will be in place to manage this risk; and

2.1.5 analysis of cost and resource implications of granting the variance.

2.2 When considering the request for a variance, the CIO may seek the input of the Information Security Governance Committee (which is the Advisory Committee defined in Policy SC14) if they consider this appropriate.

2.3 The CIO may authorize a variance from the Information Security Standards in any of the following circumstances:

2.3.1 the Administrative Head of Unit is temporarily unable to meet the compliance standard;

2.3.2 compliance is not achievable for technical or financial reasons;

2.3.3 an alternate method of compliance is available that offers equivalent or better security; or

2.3.4 the variance is otherwise reasonable and is consistent with the Information Security Standards.

2.4 If the CIO approves a deviation, they will set out the terms of the variance, including any applicable mitigation requirements or other conditions.

2.5 If the CIO denies the requested deviation, they will provide an explanation and, if possible, a suggestion of alternatives.

3. Resolution of Disagreements

3.1 If a disagreement arises and cannot be resolved in a timely manner between the CIO and the Administrative Head of Unit with respect to the requested deviation, then either party may refer the disagreement to the Responsible Executive specified under Policy SC14, who will decide the matter. This Responsible Executive may consult with the Information Security Governance Committee and/or the other Responsible Executive if they determine it would be appropriate to do so.

3.2 The Responsible Executive's decision is final.

4. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M2
User Account Management

1. Introduction

1.1 User Accounts control access to UBC Electronic Information and Systems. This document defines standards that Information Stewards/Owners must comply with when managing these accounts throughout their lifecycle to ensure individual accountability exists and access is restricted on a 'need to know' basis. In addition to this standard, Privileged Accounts must also comply with the Privileged Account Management standard.

1.2 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Creating User Accounts

2.1 Applications for User Accounts must be reviewed and approved by Information Steward/Owners and a record must be kept of all Users being granted these accounts and who provided authorization. This record must be retained for at least one year.

Examples of User Accounts

- FASmail
- Student and Alumni Email
- Student Information System (SIS)
- Financial Management System (FMS)
- Workspace
- Home network drive
- Login account (Active Directory or equivalent)

2.2 Service Providers applying for User Accounts must comply with the Outsourcing and Service Provider Management standard.

2.3 All User Accounts must be uniquely identifiable to a specific User.

2.4 Users must be granted the minimum level of access for their defined job function (i.e. the Principle of Least Privilege).

2.5 User Accounts must not be shared. Accounts must be traceable back to the individuals using them. This requirement does not apply to test accounts, which may be shared during the pre-production phase.

2.6 Where possible, User Accounts should be linked to sources of record that can accurately capture User status (e.g. Workday, PersonHub, SIS or other ERPs).

3. Changing User Account Access Rights

3.1 When Users' roles and responsibilities change, their access rights should be updated in a timely manner to ensure they remain aligned with the Principle of Least Privilege.

3.2 Changes to User Accounts should be documented, approved and retained by Information Stewards/Owners in the same manner as User Account requests.

4. Disabling User Accounts

4.1 All User Accounts must be disabled (i.e. access is revoked) in a timely manner, especially when the User has been terminated or the User has a Privileged Account. Accounts may be disabled by either closing the account to all Users or changing the password to restrict access by specific Users.

4.2 On Merchant Systems, User Accounts must be automatically disabled if not used for 90 days.

4.3 The information stored in disabled accounts, as well as the username, logs and other metadata for these accounts, must be retained for one year, except for the following accounts:

Account	Retention
Student Email	TBD, currently indefinite
Student Email Alias	TBD, currently indefinite
Home Drive	90 days

4.4 In cases where accounts are migrated from one authentication system to another, the original account does not need to be retained, provided all of the information in the account has been migrated to the new system.

4.5 At any time before the expiration of the relevant retention period, the account can be reinstated to the account holder where appropriate.

4.6 After the expiration of the relevant retention period, the account and the information stored within it must be securely deleted.

5. Reviewing User Accounts

5.1 Users' access rights must be reviewed at regular intervals to ensure they remain aligned with current roles and responsibilities. The frequency of the review must be risk based (e.g. access rights to High or Very High Risk Information such as Personal Health Information should be reviewed more frequently than access rights to Medium Risk Information that may not do as much harm if exposed to unauthorized individuals).

6. Security of User Accounts and Authentication Systems

6.1 University IT Support Staff must protect User Accounts in compliance with Securing User Accounts standard.

7. Related Documents and Resources

Privileged Account Management standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Outsourcing and Service Provider Management standard

Securing User Accounts standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M3
Privileged Account Management

1. Introduction

1.1 Privileged Accounts provide a very high degree of access to UBC Electronic Information and Systems and therefore pose a significant risk if used in an unauthorized manner.

1.2 This standard establishes requirements for the management and use of Privileged Accounts. Unless otherwise stated, Privileged Accounts are subject to the same requirements as User Accounts, as set out in the User Account Management standard. The purpose of this standard is to highlight the different or enhanced security controls that must be in place to protect Privileged Accounts.

1.3 The Administrative Head of Unit, in consultation with the Technical Owner of the UBC System is responsible for compliance with this standard.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Types of Privileged Accounts

2.1 Privileged Accounts are usually categorized into the following types:

Privileged Account Type	Description
Named Privileged Accounts	
Privileged Personal Accounts	Privileged Accounts assigned to unique individual Users (usually University IT Support Staff). Examples include the following privileged groups which Users are added to in order to elevate their privileges to the associated group access levels: DBA user, Exchange Admins, Domain Admins.
Unnamed Privileged Accounts	
Generic/Shared Administrative Accounts	Privileged Accounts that exist in virtually every device or software application; these accounts hold “super user” privileges and are often shared among University IT Support Staff. These accounts may be used by multiple Users. Examples: Windows Administrator, UNIX root, Oracle SYS, SA.
Service Accounts	Privileged Accounts that provide a security context to a running service, daemon or process, such as a file server, web server, email server, etc., or are used by applications to access databases and other applications; these accounts typically have broad access to underlying business information in databases. Also called: app2app accounts, as they are used by one application to sign into another.
Emergency Accounts	Generic Privileged Accounts used by the enterprise when elevated privileges are required for business continuity, disaster recovery, or to fix urgent problems. These accounts may be used by multiple Users. Also called: break-glass accounts, fire-call IDs.

3. Creating Privileged Accounts

3.1 Unnamed Privileged Accounts may be shared between multiple Users. However, for all privileged account types, a single individual must be assigned with accountability for the security of the account.

3.2 Approval procedures for granting access to Privileged Accounts are set out in Authorization for Privileged Account Access procedure.

4. Protecting Privileged Account Passphrases, Passwords and SSH Keys

4.1 Passphrases and passwords for Privileged Personal Accounts and Generic/Shared Administrative Accounts must be changed regularly, in compliance with the Passphrase and Password Protection

standard, or at an interval stipulated by the Technical Owner (in consultation with the Administrative Head of Unit).

4.2 Service Accounts must not be shared between applications or services, i.e. a separate account must be created for each application/service.

4.3 When private keys are used with Privileged Accounts, they must be protected in compliance with the Passphrase and Password Protection standard, except when used with Service Accounts, it is reasonable to use passphrase-less keys.

4.3.1 Private user keys must never be copied to another system than your own Workstation/personal physical disks/tokens.

4.3.2 Private machine keys must be protected as follows, except when used with Service Accounts:

4.3.2.1 the recommended settings are identical to the user keys;

4.3.2.2 the keys must be accessible only by the admin user (root) and/or the system user requiring access;

4.3.2.3 usage of machine keys should be registered in an inventory (a wiki page, LDAP, an inventory database), to allow for rapid auditing of key usage across an infrastructure;

4.3.2.4 the machine keys should be unique per usage. Each new usage (different service, different script called, etc.) should use a new, different key;

4.3.2.5 only used when strictly necessary; and

4.3.2.6 restrict privileges of the account (i.e. no root or “sudoer” machine account).

4.3.3 For additional guidance, refer to the Mozilla OpenSSH configuration document.

4.4 Passwords for Unnamed Privileged Accounts should be machine generated and held securely in a Privileged Access Management (PAM) service in compliance with the policies of the PAM service, available to system administrators in the case of an emergency through a Break Glass Procedure created by the Technical Owner (in consultation with the Administrative Head of Unit). This requirement is mandatory for Unnamed Privileged Accounts used with ERPs.

4.5 A Break Glass Procedure (which draws its name from breaking the glass to pull a fire alarm) refers to a quick means for a person who does not have access to a Privileged Account to gain access in an emergency. When a Break Glass Procedure is used, access to the Privileged Account must be:

4.5.1 limited to the minimum amount of time necessary;

4.5.2 associated to a change, problem or incident number/ticket;

4.5.3 recorded by the specific database, system, or application; and

4.5.4 logged in an auditable record (which identifies the individual User who ‘broke the glass’) for later review.

4.6 After a Break Glass Procedure has been completed, the password for the Privileged Account must be changed.

5. Logging Privileged Accounts

5.1 There are special requirements for logging Privileged Account activity, which are set out in the Logging and Monitoring of UBC Systems standard.

6. Reviewing Privileged Accounts

6.1 Access to Privileged Accounts must be reviewed at an interval stipulated by the Technical Owner of the UBC System (in consultation with the Administrative Head of Unit), or at a minimum annually, to validate that they remain restricted to authorized personnel. Discrepancies must be reported in a in a timely manner to the Technical Owner for resolution.

7. Responsibilities of Users with Access to Privileged Accounts

7.1 As Privileged Accounts provide a significant level of control over UBC Electronic Information and Systems, individuals with access to these accounts are expected to exercise a higher degree of caution than for User Accounts.

7.2 All Users with access to Privileged Accounts must maintain the confidentiality of any information that they have access to both during, and after, their employment with UBC.

7.3 All Users with access to Privileged Accounts:

7.3.1 must not use Privileged Accounts for day-to-day activities, such as email and web browsing;

7.3.2 wherever possible, must not use Privileged Accounts (except Service Accounts) to run daemons, services or applications.

7.4 University IT Support Staff with access to Privileged Accounts, and all IT professionals must also comply with the System Administrators' Code of Ethics.

8. Related Documents and Resources

User Account Management standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Authorization for Privileged Account Access procedure

Passphrase and Password Protection standard

Mozilla OpenSSH Guidance

Logging and Monitoring of UBC Systems standard

System Administrators' Code of Ethics

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M4
Securing User Accounts

1. Introduction

1.1 User Accounts control access to UBC Electronic Information and Systems and as such they must be effectively protected against unauthorized access. This standard is closely tied to the User Account Management standard.

1.2 This document defines standards that University IT Support Staff must comply with when securing these accounts.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Account Protection Requirements

2.1 All User Accounts must be secured with:

2.1.1 passphrases or passwords that are in compliance with the Passphrase and Password Protection standard; or

2.1.2 private keys (e.g. X.509 certificates or SSH Keys) that are generated using, at a minimum, the Mozilla Key Management Acceptable algorithms, but wherever possible, should use the Recommended algorithms.

2.2 Where technically possible, UBC Systems must enforce password complexity rules in accordance with the Passphrase and Password Protection standard.

2.3 Where technically possible, Servers and Software Applications must be protected by Multi-Factor Authentication (MFA).

2.4 Users who receive new accounts or who require a replacement password must be forced to set or change the password upon first login. Account activation or password reset links, and temporary passwords must be transmitted to Users in a secure manner and expire as follows:

Credential Change	Initiated by	Link/Password Expiration	Examples
Account Activation	Administrator or automated process	7 days	New employees, sponsored guests and prospective student accounts
	User (self-serve sign-up)	3 days	New and prospective student accounts
Password Recovery	User (self-serve)	24 hours	Applies to all Users

2.5 Procedures must be established to verify the identity of a User prior to providing a new, replacement or temporary password for an account. Identification validation procedures must follow one of the following standard practices, listed in order of preference:

2.5.1 MFA application push to the User's Multi-Factor Authentication Device (MFA Device) that must be approved by the User;

2.5.2 Validation of the answers to three questions that were previously created by the User during account creation; or

2.5.3 In-person visit by the User to present valid photo identification, preferably University or government-issued.

2.6 Default vendor passwords must be changed following the installation of systems or software.

3. Authentication System Requirements

3.1 Where possible, all User Accounts should be centrally controlled in the UBC Enterprise Active Directory, Enterprise LDAP, or Campus-wide Login.

3.2 Authentication systems for User Accounts must be adequately protected from password cracking using at least one of the following methods:

3.2.1 the account is locked for a period of time if an incorrect number of passwords/passphrases is entered over a specified time period (for example, if an incorrect password/passphrase is entered 10 times within a 30 minute window, the account will be locked for 30 minutes); and/or

3.2.2 each time an incorrect password/passphrase is entered, the system introduces a delay before providing the failure response; this delay increases as the failed login attempts continue but will reset once the User successfully logs in (for example, the delay period could begin at 100 milliseconds, and double after each subsequent failed login).

3.3 Authentication systems must not store account passwords in clear text. Where possible, passwords should be stored using a strong cryptographic hash and salted; for further guidance see Salted Password Hashing – Doing it Right.

3.4 Where possible, authenticated application sessions must timeout as follows, after which Users must reauthenticate to continue an existing session or establish a new session:

3.4.1 after a maximum session length of 12 hours; and

3.4.2 where reasonable, after 30 minutes of User inactivity.

4. Related Documents and Resources

User Account Management standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Passphrase and Password Protection standard

Mozilla Key Management document

Salted Password Hashing

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M5
Vulnerability Management

1. Introduction

1.1 This document defines standards for protecting UBC Systems through vulnerability management, which is a security practice designed to proactively reduce the chance of exploitation of IT vulnerabilities. Effective vulnerability management includes patch management, vulnerability scanning, vulnerability mitigation, malware protection and secure configuration of systems, particularly firewalls. Unless otherwise stated in this standard, vulnerability management is the responsibility of University IT Support Staff.

1.2 This standard applies to UBC Systems containing Medium, High or Very High Risk Information, and may also be applied to UBC systems containing Low Risk Information where appropriate.

1.3 University IT Support Staff with access to Privileged Accounts, and all IT professionals must also comply with the System Administrators' Code of Ethics.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Patch Management

2.1 University IT Support Staff are responsible for subscribing to the Appropriate Notification Services to ensure they are aware of new vulnerabilities and corresponding patches as soon as they are available.

2.2 Patch management procedures must prioritize patches based on the severity of the vulnerability being patched, the sensitivity of the data in the system, and the criticality of the system to University Business. For additional guidance on patching prioritization, refer to the Vulnerability Awareness & Patching Prioritization guide. A back-out or roll-back procedure should also be in place so that the patch can easily be removed in the event of a serious problem.

2.3 Backups should be completed before applying any significant patches, in case of unexpected problems.

2.4 Operating system and application updates/patches must be installed as follows:

2.4.1 to the extent possible, desktops, laptops and servers must be configured to install these updates and patches automatically;

2.4.2 where automatic installation is not feasible, all security-related updates and patches must be manually installed at the earliest opportunity, in accordance with their severity, as outlined in section 2.5 below;

2.4.3 where it is impractical or impossible to install security-related updates and patches, the risks must be mitigated with compensating controls approved by the CISO; and

2.4.4 where the system is at end of life and security-related updates and patches are no longer available from the vendor, then you must either upgrade the system or implement compensating controls approved by the CISO.

2.5 Unpatched software is frequently exploited by malicious individuals to access information or resources. To mitigate this threat, vendor provided patches for UBC Systems (e.g. operating systems, applications, databases, etc.) must be patched, with service outages where required, in accordance with Severity Ratings for Vulnerabilities (CVSS) or as defined by the vendors or other third parties as follows:

2.5.1 Critical-Severity Vulnerabilities as soon as possible, preferably within 72 hours of the patch release;

2.5.2 High-Severity Vulnerabilities as soon as possible, preferably within 14 days of the patch release; and

2.5.3 Medium-Severity Vulnerabilities as soon as possible once all Critical and High-Severity Vulnerabilities have been resolved.

2.6 Instrumentation systems that are network-connected and run Windows embedded operating system or any other embedded operating system that can only be patched by the hardware vendor are examples of IoT Devices or appliances (including virtual appliances), and frequently will have vulnerabilities for which there are no patches to protect the system. In this case, it is important to look at compensating controls, which will protect the system and reduce the risk of unauthorized access to information or resources. A possible compensating control may be to isolate the system, so that it has no access to the internet or other systems, with the exception of a "proxy" system. The proxy system will be able to access other computers and the internet and through a dedicated interface, it can communicate with the system. Provided the proxy system can be well patched and secured, the risk of access to the unpatched system is reduced to a reasonable level by this control. For additional information on securing IoT Devices, see the Securing Internet of Things (IoT) Devices standard.

3. Vulnerability Scanning

3.1 The Office of the CIO is responsible for ensuring that all operational UBC Systems attached to the UBC network are scanned with a network vulnerability scanning tool (e.g. Nessus) at least every quarter.

3.2 The Office of the CIO is responsible for scanning Web Applications on UBC Systems attached to the UBC network with a web application scanning tool.

3.3 University IT Support Staff have the responsibility to obtain a vulnerability scan for all new or substantially modified Internet-facing servers and applications attached to the UBC network prior to going into production. Any detected vulnerabilities must be resolved in accordance with their severity, as outlined in section 2.5 above; rescans are required until passing results are obtained.

3.4 University IT Support Staff must not block UBC's Vulnerability Scanners.

4. Penetration Testing

4.1 It is highly recommended that Penetration Testing be conducted for UBC Systems containing or processing High or Very High Risk Information. To find a qualified penetration testing service, contact information.security@ubc.ca.

5. Malware Protection and Hardening

5.1 Anti-malware software protects against malicious code and is another layer of defense to help protect against exploitation of vulnerabilities.

5.2 Desktops, laptops and servers connected to UBC's network or other networked resources must have anti-malware software installed and configured, so that the virus definition files are updated daily. The anti-malware software must be actively running on these devices and kept up-to-date.

5.3 Unused services on servers should be disabled, and operating systems and applications should be hardened against external threats, see the UBC Systems and Applications Hardening Guides for recommended configurations.

5.4 Applications should be appropriately hardened against attacks. For configuration guidance on your specific application, see the Mozilla Observatory. For additional help, contact UBC Cybersecurity.

6. Firewall Configuration

6.1 Firewalls provide an effective compensating control for many types of vulnerabilities for which patches are not readily available; these are known as zero-day vulnerabilities. UBC Systems storing Medium, High or Very High Risk Information must be protected by a firewall.

6.2 Firewalls are only as effective as their Access Control List (ACL) rule set, which determines how traffic is blocked or passed. Firewall ACL rule sets must be configured as follows:

6.2.1 a "Deny by Default" policy must be implemented on all firewalls;

6.2.2 services that are not explicitly permitted must be denied;

6.2.3 firewalls must use ingress filtering at a minimum and must use egress filtering if it is used to protect High or Very High Risk Information;

6.2.4 ACLs must restrict traffic to the minimum necessary to conduct University Business; and

6.2.5 rule sets must be reviewed annually for optimization and validation of effective rules.

6.3 Network-based firewalls configured to control access to different zones must be dedicated firewalls. Firewalls should never be used for multiple purposes beyond access control and monitoring. Next Generation firewalls, Unified Threat Management (UTM) and virtual firewalls are still considered to be dedicated.

6.4 Where high availability is required, standby firewalls should be configured to take over the services of primary firewalls in the event that the primary fails. This also implies that standby firewalls must be kept up to date with changes made to the primary firewall to properly support this capability.

6.5 If a firewall becomes a single point of failure, it must fail in a closed state and not allow passage of data traffic through it.

6.6 The firewalls must be capable of “stateful packet inspection” and this capability must be turned on.

6.7 All firewall critical alarms must generate an automatic notification to the firewall administrator.

6.8 Host based firewalls should be used if available, in addition to network firewalls; this facilitates defense in depth.

6.9 All firewall logs should be sent to a separate machine solely dedicated to the collection of logs at an appropriate level.

7. Related Documents and Resources

System Administrators’ Code of Ethics

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Appropriate Notification Services guideline

Vulnerability Awareness & Patching Prioritization *(with CWL credentials)*

Severity Ratings for Vulnerabilities (CVSS)

Securing Internet of Things (IoT) Devices standard

UBC’s Vulnerability Scanners *(with CWL credentials)*

UBC Systems and Applications Hardening Guides

Mozilla Observatory

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M6
Security of Wi-Fi Infrastructure

1. Introduction

1.1 UBC has a large and complex Wi-Fi network that plays an integral role in the operations of the University. Consequently, intruders and hackers may consider the Wi-Fi network an attractive target to breach the security of UBC Electronic Information and Systems.

1.2 This standard defines requirements to ensure that Wi-Fi devices, such as Wireless Access Points (WAPs), which allow Wi-Fi devices to connect to a wired network, are deployed in a secure, controlled and centrally managed way to reduce the likelihood of a security breach. Unless otherwise indicated, the UBC IT NETwork and Infrastructure Team is responsible for ensuring compliance with this standard. This policy applies to areas where WAPs installed by UBC IT provide Wi-Fi coverage.

1.3 In addition to this standard, UBC IT Wi-Fi networks provisioned by UBC IT are governed by Policy SC11, Management of the Wireless Network.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Deployment of WAPs

2.1 All deployment of WAPs must be authorized by UBC IT.

2.2 WAP hardware must be protected to ensure physical security mechanisms (e.g. locked cabinet, high ceiling mount, etc.) are in place to prevent theft, alteration, or misuse.

3. Secure Configuration

3.1 All WAPs should be secured using a minimum of Wi-Fi Protected Access (WPA2) with a minimum of AES 128-bit encryption.

3.2 Wired Equivalent Privacy (WEP) is prohibited for Wi-Fi network security, as it is insecure.

3.3 It is recommended that Users connecting to WAPs, providing access to the UBC LAN, be configured to use the "AutoConnect" ubcsecure automated client configuration tool. This will help prevent connecting to rogue WAPs, which have been setup with the same name (spoofing) to steal credentials.

3.4 Console access must be password protected in compliance with the Passphrase and Password Protection standard.

3.5 WAP and wireless controller management must be handled as follows:

3.5.1 utilize secure protocols such as HTTPS, SSH, and CAPWAP;

3.5.2 management must only be over the LAN interface;

3.5.3 if SNMP is used in the management environment, all default SNMP community strings must be changed, otherwise it must be disabled;

3.5.4 vendor defaults such as encryption keys, and administrative passwords must be changed.

3.6 The use of Telnet or other insecure protocols is prohibited.

4. Security Updates

4.1 The operating system or software code on WAP and wireless controllers should be patched and kept current to ensure proper protection from the latest security vulnerabilities.

4.2 WAPs and wireless controllers must be replaced if they have reached end of life for software support.

5. Additional Requirements for Merchant Systems

5.1 Users responsible for Merchant Systems must:

5.1.1 ensure that a perimeter firewall is in place between any Wi-Fi network and Merchant Systems processing Payment Card Industry (PCI) Information. These firewalls must be configured to deny or control any traffic from the Wi-Fi environment to Merchant Systems;

5.1.2 test for the presence of unauthorized WAPs on a quarterly basis. Note: Methods that may be used in the process include, but are not limited to, Wi-Fi network scans, physical/logical inspections of system components and infrastructure, network access control NAC), or Wi-Fi IDS/IPS; and

5.1.3 report any unauthorized WAPs as a security incident, in compliance with the Reporting Information Security Incidents standard.

Related Documents

Policy SC11, Management of the Wireless Network

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

UBC IT AutoConnect Secure Wireless Setup

Passphrase and Password Protection standard

Reporting Information Security Incidents standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M7
Cryptographic Controls

1. Introduction

1.1 This document defines standards for the implementation and use of encryption technologies within UBC to maintain the confidentiality and integrity of UBC Electronic Information. For standards on when encryption is required, see the Encryption Requirements standard.

1.2 Cryptographic controls provide an enhanced level of protection for UBC Electronic Information in the event of theft, loss or interception by rendering information unreadable by unauthorized individuals. Unless otherwise stated, University IT Support Staff are responsible for ensuring compliance with this standard.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Cryptographic Requirements

2.1 Encryption usage must be risk based and must take into account the sensitivity of information as per the Encryption Requirements standard.

2.2 Encryption strength must be AES-128 bit or equivalent, at a minimum; AES-256 bit encryption is preferred as it provides greater protection.

2.3 Cryptographic hash ciphers must be strong: SHA256, SHA512, RipeMD-160, WHIRLPOOL or equivalent, and weak cryptographic hash ciphers must be disabled.

2.4 Whenever a password or passphrase is used as an encryption key ("Key"), it must follow the standards defined in the Passphrase and Password Protection standard, which details strong password/passphrase construction. Keys that are compromised (e.g. lost or stolen) must be reported immediately in accordance with the Reporting Information Security Incidents standard. The Key must be revoked or destroyed and a new key generated. Key re-assignments require re-encryption of the data.

2.5 Digital signatures should be supported by certificates issued by a trusted third party Certificate Authority (CA); if the signatures are intended for legal signing then they must be supported third party CA certificates. The minimum acceptable hash algorithm is SHA2; SHA0 and SHA1 cannot be used as they are insecure.

2.6 The following requirements apply to X.509 certificates:

2.6.1 X.509 certificates used for the securing of Medium, High or Very High Risk Information during User transmission must be issued by a trusted third party CA, as part of a Public-Key Infrastructure (PKI);

2.6.2 server-to-server transmissions should be encrypted and should use a trusted third party certificate;

2.6.3 newly purchased or renewed X.509 certificates must be a minimum of 2048-bits; and

2.6.4 X.509 certificates may be purchased under the University's Enterprise account, via security@ubc.ca.

3. Full Disk Encryption (FDE)

3.1 For additional requirements around FDE, see the Encryption Requirements standard.

4. Key Management

4.1 For encryption to be effective, encryption Keys must be protected against unauthorized disclosure, misuse, alteration or loss. In order to reduce the risk of loss or exposure of Keys, it is recommended that all Key management processes be performed with automated software. A Key management plan must also be in place that covers the following process areas:

Process Area	Process Description	Process Requirements
Key Generation	Secure creation of keys (symmetric encryption) or key pairs (asymmetric encryption).	• Keys must be created using cryptographically strong algorithms (see Cryptographic Requirements above).
Key Distribution	Secure distribution of keys using manual transport methods (e.g. file transfer, key loaders), automated methods (e.g. Key transport and/or Key agreement protocols), or a combination thereof.	• Keys must be encrypted when transmitted over communication lines. • The exchange of keys must employ encryption using an algorithm that is at least as strong as the one that is used to encrypt the data protected by the keys, and access must be strictly limited to those who have a need-to-know.
Key Storage and Protection	Protect all cryptographic keys against modification, loss and destruction.	• Keys and their associated software products must be securely maintained for the life of the archived data that was encrypted with that product. • Keys must be protected using the same or superior level of security as the information that they are protecting, and access must be strictly limited to those who have a need-to-know. • In public-private key encryption, private keys need protection against unauthorized disclosure. • Keys must not be stored on the same storage media as the encrypted data. • Equipment used to generate, store and archive keys must be physically protected.
Key Recovery	To prevent data loss, establish processes to ensure Keys can be recovered if they are forgotten.	• Strategies must be implemented to enable Key recovery. • UBC's central Key Escrow services are recommended for this purpose because they are reliable and secure. • See the Key Escrow guideline for additional information. • The recovery process must be documented to assure it will be effective when required.
Key Change	Revoke and publish new keys when they are suspected of compromise or unauthorized disclosure, they reach the end of their lifetime, and/or the key owner or delegated individual leaves the employ of UBC.	• Key lifespan must be documented along with processes and rules for making changes to keys. • Clear authorization process for key changes. • Specific responses to suspected compromised keys.

5. Additional Requirements for Merchant Systems

5.1 Users must not store authentication data collected in Merchant Systems after authorization (even if this data is encrypted). Authentication data includes:

5.1.1 the full contents of any track from the magnetic stripe or chip;

5.1.2 the card-verification code or value (three or four-digit number printed on the back/front of a payment card); and

5.1.3 the personal identifier number (PIN) or the encrypted PIN block.

5.2 Users must ensure that the credit card number is masked (the first six and last four digits are the maximum that can be displayed) whenever displayed (e.g. electronically, hard-copy, etc.).

6. Related Documents and Resources

Encryption Requirements standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Passphrase and Password Protection standard

Reporting Information Security Incidents standard

Key Escrow guideline

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M8
Logging and Monitoring of UBC Systems

1. Introduction

1.1 Effective logging and monitoring procedures (i.e. continual monitoring and/or periodic reviews) provide ongoing assurance that UBC Systems and the UBC Electronic Information that they hold are secure, and that confidentiality and integrity are effectively being ensured. In the event of a security breach, audit logs are relied upon to determine whether or not information has been accessed or modified without authority.

1.2 The nature and frequency of logging and monitoring procedures must be based upon the sensitivity of the information stored in the system and the potential impact of a security breach upon the University and affected individuals. It is only necessary to implement logging and monitoring at a level that will reasonably identify unauthorized access to UBC Systems and UBC Electronic Information in a timely manner. Logging and monitoring should be considered at the operating system, database and/or application level.

1.3 This standard defines requirements for effective logging and monitoring of UBC Systems and UBC Electronic Information for security purposes. Unless otherwise stated in this document, University IT Support Staff are responsible for ensuring compliance with these standards. In addition, Information Stewards/Owners are responsible for ensuring that logging and monitoring procedures are adequate for securing the information they are responsible for. ERPs, Merchant Systems and EMRs must be compliant with this standard; it is recommended that all other UBC Systems comply with this standard.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Logging and Monitoring Requirements

2.1 The following key activities must be logged:

2.1.1 User login, logout and access to a resource;

2.1.2 action performed by the User and the time it was performed; and

2.1.3 where feasible, any access to, or modification of, records.

2.2 Logs should be configured to record system faults that are potential indicators for detecting attacks against UBC Systems or other unauthorized activity.

2.3 Logs provide valuable information that can be used to validate the integrity and confidentiality of UBC Electronic Information; to be effective, logs must be:

2.3.1 retained for at least 90 days (except for ERP logs, which must be retained for at least 365 days) and regularly backed up whenever possible, preferably to offsite secure storage;

2.3.2 retrievable in a timely manner if they are required for analysis; and

2.3.3 protected against unauthorized access and modification, preferably by locating them on a separate server outside the Demilitarized Zone (DMZ), such as a Database Server protected by a firewall, and restricting access as necessary; no-one should be able to change or delete log information.

2.4 Logs should be monitored to determine the use of system resources and to detect information security events (e.g. failed logons, simultaneous logins from different geographic locations, escalation of privilege, attacks against systems, etc.). Monitoring software should be configured to send an alert to responsible University IT Support Staff when appropriate.

2.5 Accurate logs are dependent on accurate time. Systems containing or processing High or Very High Risk Information must be set to synchronize their clocks with a reliable source. UBC's DNS servers act as the University's (Time synchronization) NTP servers. These are synchronized to an external time source, ntp.org; all Users and University IT Support Staff should use these or an equivalent service as a time synchronization source. More details on this service can be found on the myDNS Overview page.

3. Additional Requirements for Privileged Accounts

3.1 University IT Support Staff must ensure that logs are kept of the usage of all Privileged Accounts. Key activity to be logged must include the following:

3.1.1 login, logout and the identity of the User, if known;

3.1.2 action performed and the time it was performed;

3.1.3 where feasible, any access to, or modification of, UBC Electronic Information; and

3.1.4 any other information that the Information Stewards/Owners decide should be captured in order to protect high risk files.

3.2 Logs of Privileged Account activity must be reviewed on a regular basis to detect information security events and determine if further investigation is required; where feasible this should be automated. Investigations should be reported to the Information Steward/Owner as required.

3.3 Where appropriate, Privileged Account logging systems must automatically transmit alerts of significant activities to the technology owner (typically a manager of a University IT Support Staff team). The following activities must always trigger an alert:

3.3.1 escalation of privilege; and/or

3.3.2 usage of the Break Glass Procedure as described in the Privileged Account Management standard.

4. Additional Requirements for Merchant Systems

4.1 For all Merchant Systems processing PCI Information, there is a requirement that logs be maintained for the following events:

4.1.1 which particular record was accessed;

4.1.2 which User accessed the record; and

4.1.3 the time the User accessed the record.

4.2 Logs of access to PCI Information should be retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

5. Use and Disclosure of Logs

5.1 Logs are generally intended to be used for maintenance and troubleshooting, as well as detecting and investigating information security events. Access for other purposes must be approved using one of the following methods:

5.1.1 internally, within UBC, in accordance with the Accessing Electronic Accounts and Records standard;

5.1.2 externally to law enforcement via Campus Security; or

5.1.3 externally to other entities via authorization from the Office of the University Counsel.

6. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

UBC IT myDNS

Privileged Account Management standard

Accessing Electronic Accounts and Records standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M9
Physical Security of UBC Datacentres

1. Introduction

1.1 Effective security measures require physical security controls. While electronic controls alone are important, they may become useless if the device is physically accessed or removed by an unauthorized party.

1.2 This document defines standards for the physical security of UBC Datacentres. These Datacentres are intended to provide a secure location for operations, controlled access to equipment and data, protection against environmental threats and support for the availability requirements of UBC Electronic Information and Systems. University IT Support Staff are responsible for ensuring that the requirements of this document are complied with.

1.3 The University has a responsibility to protect High and Very High Risk Information from unauthorized viewing and use. In particular, the BC *Freedom of Information and Protection of Privacy Act* (FIPPA)[1] and Policy GA4, Records Management[2] require public bodies to implement reasonable and appropriate security arrangements for the protection of Personal Information (in both electronic and paper format). Therefore, servers containing significant quantities of High or Very High Risk Information must be hosted in UBC Datacentres or in third party servers that have an equivalent level of security to this standard. Where appropriate, Low and Medium Risk Information may also be hosted in UBC Datacentres.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Physical Security Controls

2.1 The table below outlines the minimum set of physical security controls required for UBC Datacentres, based upon the Security Classification of UBC Electronic Information standard.

Control Area	Information Security Classification			
	Very High Risk	High Risk	Medium Risk	Low Risk
Rooms	Datacentre must be located in a fully enclosed room. Walls must meet the following criteria: • Must extend from floor to ceiling slab. • Should preferably be constructed from a solid, resistant material such as concrete or brick. If they are not solid (e.g. drywall), then they must be reinforced with wire mesh.			Equipment can be located in open areas if other protective measures are in place, e.g. locked cages.
Doors and Locks	• Datacentre doors must be locked when room is not in use. • Good practice is to install automatic closing mechanisms. • Security grade door fastening hardware must be used in conjunction with a metal door and frame. • Acceptable locking mechanisms include electronic proximity access cards/fobs, keypad type entry locks, and biometric locks.			Datacentre doors must be locked when room is not in use. Either electronic or mechanical locks are acceptable.
Glazing	All exterior glass in doors and accessible windows must be reinforced. Consider installing high-grade security film (minimum standard should be Profilon AXA1-15Mil or equivalent) to resist forced entry.			Windows must be able to securely lock from the inside.

[1] FIPPA, section 30
[2] Policy GA4, section 2.4

Control Area	Information Security Classification			
	Very High Risk	High Risk	Medium Risk	Low Risk
Visibility of Equipment	Window coverings (blinds/shades) or reflective/tinted film should be installed on glazed windows or doors in order to reduce direct sightlines to valuables inside the facility.			
Cabling	Power and network cabling carrying data or supporting information services should be protected from interception or damage outside of the Datacentre.			
Managing Access	• The public must not have direct access to the Datacentre perimeter. An outer security perimeter should be established with access controls sufficient to prevent direct public access. • Use signage to clearly delineate publicly accessible space from Authorized Personnel-Only areas. Signage should not indicate the presence of UBC Electronic Systems. • Individual(s) must be assigned the authority to grant access to the Datacentre and someone must be appointed to formally manage the physical access process including revocation of access (fob/card, keypad access). • Individuals who are not authorized to access the Datacentre must be escorted at all times by an authorized individual • Access must be logged electronically or in a logbook in the case of keypad entry doors that do not uniquely identify an individual.			
Alarms and Remote Monitoring	Alarms (monitored 24/7) must be installed that trigger on unauthorized access.		Good practice is to install and monitor an alarm system to detect intruders.	
	CCTV has been debated as an effective deterrent to crime, but if employed with adequate resolution and proper camera placement, its forensic effectiveness is undisputed. All CCTV installations must be approved by the Access and Privacy Manager.			
Power Supply	• Redundant power should be supplied to the Datacentre where possible. • Servers should all be connected through a UPS in order to remain running in the event of short power outages.			n/a
Environmental Controls	• Sufficient Heating, Ventilation and Air Conditioning (HVAC) systems must be in place to effectively maintain all UBC Electronic systems within the manufacturers' required temperature and humidity operating ranges. • Measures must be in place to monitor and detect variation in temperature and humidity • Where possible, water and drainage plumbing should not run across the ceiling of a Datacentre. • The floor of the Datacentre should be raised above the subfloor to reduce the risk of flood damage.			Comply with Building Code requirements.
Fire Protection	Fire detection and suppression devices, such as fire extinguishers and pre-action or dry pipe sprinkler systems, must be in place.			Comply with Building Code requirements.
Data Backups	If information is backed up onto electronic media, the same physical security requirements are to be applied to that media unless the information is encrypted (see the Encryption Requirements standard).			

3. Related Documents and Resources

BC Freedom of Information and Protection of Privacy Act (FIPPA)
Policy GA4, Records Management
Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Security Classification of UBC Electronic Information standard
Encryption Requirements standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M10
Internet-facing Systems and Services

1. Introduction

1.1 UBC Systems and services that are Internet-facing (i.e. visible or accessible from the Internet) are prime targets for exploitation. Without adequate security, these systems and services provide an avenue for malicious activity such as theft of UBC Electronic Information or the denial of service to UBC resources.

1.2 This document defines minimum standards to be followed by University IT Support Staff for the security architecture, protected network protocols, hardening/patching and monitoring/logging of UBC's Internet-facing systems and services to ensure they are adequately protected. This standard focusses on Web Servers because these are primary targets for exploitation and therefore pose the highest risk to the University. Servers that are not Internet-facing, such as intranet servers, should also follow this standard, wherever feasible.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Security Architecture Requirements

2.1 Ideally, web, application and database functions should be hosted on separate servers; however, it is acceptable to host all of these functions on the same server in the following circumstances:

2.1.1 High or Very High Risk Information is not being processed through these servers; and/or

2.1.2 hosting the functions on separate servers would not be technically feasible or would cause unreasonable business disruption (e.g. render the application unusable or unsupportable).

2.2 If functions are hosted on the same server, compensating controls must be implemented to commensurate with the risk, such as:

2.2.1 web application (layer 7) firewall;

2.2.2 file integrity monitoring;

2.2.3 Intrusion Detection Systems/Intrusion Prevention Systems; and

2.2.4 log monitoring (e.g. SIEM).

2.3 When web, application and database functions are hosted on separate servers, Web Servers are permitted to communicate with Application Servers but not with Database Servers.

2.4 All Internet-facing servers must be placed in a Demilitarized Zone (DMZ) configured as follows:

2.4.1 the DMZ must contain all Web Servers;

2.4.2 the DMZ may only contain Application Servers if they are combined with Web Servers;

2.4.3 the DMZ must not contain Database Servers that store or process High or Very High Risk Information;

2.4.4 a firewall must be in place between the DMZ and the Internet as well as between the DMZ and the UBC internal network;

2.4.5 wherever possible the DMZ should be protected from the Internet by web application firewalls, as they are better equipped to protect web applications from threats;

2.4.6 firewalls must use ingress filtering at a minimum, and must also use egress filtering if the firewall is used to protect High or Very High Risk Information; and

2.4.7 firewalls must use access rules that restrict traffic to only the minimum necessary to conduct University Business; access rules must not be wide-open allowing any source to connect to any destination, as this defeats the security of the firewall.

2.5 Access to all Medium, High and Very High Risk Information on servers must be authorized and limited based on the User's role, following the Principle of Least Privilege.

3. Network Protocol Requirements

3.1 Secure transmission of Medium, High or Very High Risk Information must comply with the following requirements:

3.1.1 any form, application or service that requires some type of authentication, or that is used to collect or transmit information from User to server or between servers, must be encrypted using HTTPS with TLS version 1.2 at a minimum (or the equivalent, for non-web-based applications);

3.1.2 information transmitted via SSH must be encrypted using a minimum of AES-256 bit encryption with mutual authentication between the server and User; and

3.1.3 known weak network protocols (e.g. all versions of SSL, and TLS versions prior to 1.2) should be disabled.

3.2 Secure transmission of Low Risk Information is strongly recommended to be encrypted using HTTPS with TLS version 1.2 at a minimum.

3.3 Where HTTPS is used, it is recommended that all HTTP requests are re-directed to HTTPS.

3.4 Users frequently access desktops, laptops and servers remotely. Remote Access covers a broad range of technologies, protocols and solutions (e.g. RDP, SSH, VNC, VDI, terminal services, etc.). Remote Access must comply with the following requirements, where possible:

3.4.1 Multi-Factor Authentication (MFA) must be used;

3.4.2 remote access servers (e.g. terminal server, VDI, Remote Access Gateways, etc.) must be located in the DMZ and use strong encryption for server-to-User transmissions, e.g. RDP with Network Level Authentication, SSH with AES-256 bit encryption, etc.;

3.4.3 host desktops, laptops or servers not located in the DMZ must be remotely accessed via a Remote Access Gateway, VPN or SSH; and

3.4.4 VPN connections must be encrypted and restricted at both ends to the minimum number of systems necessary. To support this:

3.4.4.1 DNS or service-based split tunneling (e.g. Dynamic Split Tunneling) may be used with authorization of specific services by the CISO;

3.4.4.2 IP or subnet-based split tunneling must not be enabled; and

3.4.4.3 Local LAN access may be enabled with authorization by the CISO.

3.5 Servers running other Internet-facing protocols must be located in the DMZ and must encrypt transmissions of Medium, High or Very High Risk Information.

4. Additional Requirements for Merchant Systems

4.1 University IT Support staff must configure Remote Access technologies used in Merchant Systems to automatically disconnect User sessions after a specific period of inactivity. 30 minutes is recommended.

5. Hardening and Patching Requirements

5.1 Servers must be hardened, patched and scanned in accordance with the Vulnerability Management standard.

6. Logging and Monitoring Requirements

6.1 Servers must be logged and monitored in accordance with the Logging and Monitoring of UBC Systems standard.

7. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Vulnerability Management standard

Logging and Monitoring of UBC Systems standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M11
Development and Modification of Software Applications

1. Introduction

1.1 When purchasing, designing or substantially modifying Software Applications, it is important that security requirements are understood, documented and implemented at the earliest appropriate stage of the project. This is substantially cheaper and more effective than trying to apply security controls retroactively.

1.2 Information Stewards/Owners are responsible for ensuring this standard is complied with whether the project is undertaken internally or by a Service Provider.

1.3 The Chief Information Officer has issued this document under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Assessing Security Requirements for Projects Involving Medium, High or Very High Risk Information

2.1 Prior to storing or accessing UBC Electronic Information, complete a Software Application Security Checklist for all new or substantially modified applications that store or access Medium, High or Very High Risk Information.

2.2 All new or substantially modified applications that store or access Personal Information must also undergo a privacy impact assessment (PIA), as set out in the Privacy Impact Assessment Requirements. This PIA may require additional security assessments.

Examples of "Substantially Modified":

- granting access privileges to Medium, High or Very High Risk Information to new categories or groups of individuals
- outsourcing management, storage or security of Medium, High or Very High Risk Information to an external service provider
- changing how Medium, High or Very High Risk Information is collected, used or displayed

3. Pre-Production Development and Test Environments

3.1 Development and test environments must be logically and/or physically isolated from any production environments.

3.2 Where possible, testing of new applications should be done with fabricated data that mimics the characteristics of the real data, or on copies of real data with any Medium, High or Very High Risk Information appropriately sanitized. Testing should not be done on live data due to the threat to its confidentiality and/or integrity. Testing that requires the use of live data or High/Very High Risk Information must have appropriate security controls employed.

4. Application Development Requirements

4.1 Applications must validate input properly and restrictively, allowing only those types of input that are known to be correct (e.g. cross-site scripting, buffer overflow errors, SQL injection flaws, etc.).

4.2 Applications must execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system. See the Open Web Application Security Project for more information.

4.3 Where possible, code-level security reviews must be conducted with professionally trained peers for all new or significantly modified applications, particularly, those that affect the collection, use, and/or display of High or Very High Risk Information.

4.4 All new or substantially modified applications connected to the UBC network must be scanned for vulnerabilities in accordance with the Vulnerability Management standard.

5. Naming Requirements for Web Applications

5.1 Web Applications used to conduct University Business must be provisioned within the ubc.ca domain name space, e.g. widget.ubc.ca, unless not technically possible.

6. Email Requirements for Applications and ERPs

6.1 Due to the high risk of fraud and account compromise, ERPs must adhere to the following:

6.1.1 The inclusion of clickable links in unsolicited emails generated from ERPs is prohibited. In emails that are requested by the recipient, the inclusion of clickable links is not recommended. Instead, instruct Users to navigate to the ERP or website directly.

6.1.2 Use of the svc.ubc.ca managed mail subdomain service is required for all ERPs, e.g. widget.svc.ubc.ca.

6.2 The requirements in section 6.1 should be applied to non-ERP Applications unless not technically possible.

6.3 In order to make emails generated from Applications and ERPs more difficult to replicate, follow these guidelines where possible:

6.3.1 use a UBC-branded email template and remove vendor branding;

6.3.2 use customized language specific to the required action, or that defines a specific set of activities;

6.3.3 consider adding a named email signatory; and

6.3.4 include authenticating context, e.g. by providing salutations to the recipient.

7. Change Management

7.1 A change management process must be implemented and maintained for changes to existing applications; substantial modifications may trigger a new assessment of security and privacy risks, as explained above.

8. System Documentation

8.1 University IT Support Staff must securely store system documentation and ensure that it is only available to authorized Users.

9. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Software Application Security Checklist

Privacy Impact Assessment (PIA)

Open Web Application Security Project (OWASP)

Vulnerability Management standard

Application Security Guidelines (with CWL credentials)