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 of Direct Attached Storage (DAS)

6.1 External Direct Attached Storage (DAS) and Servers that have internal DAS are exempt from encryption requirements if they meet the criteria in the Encryption Exemption for Direct Attached Storage with Low Risk Information checklist. The completed checklist must be submitted to information.security@ubc.ca.

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

How to Encrypt Files Using Common Applications guideline

Transmission and Sharing of UBC Electronic Information standard

Encryption Exemption for Direct Attached Storage with Low Risk Information checklist

Passphrase and Password Protection standard

Cryptographic Controls standard