a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #05
Encryption Requirements

Introduction

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 to safeguard UBC Electronic Information when they are accessing it for University Business purposes. This standard may also be used to protect the User's own personal data, e.g. personal banking information.
2. This standard incorporates the legal requirement to encrypt Personal Information stored on a laptop or a mobile Device, which has been affirmed by the British Columbia Information and Privacy Commissioner in their interpretation of the *Freedom of Information and Protection of Privacy Act*.
3. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Password Protection and Zipping

4. 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.
5. 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.

Device-Level Encryption Requirements

6. Encryption requirements apply to devices that are used for University Business. Wherever possible, encryption should be implemented at the Device level, as follows:

Device Types	Encryption Requirements	Recommended Toolset
Mobile Devices		
Laptops	Full disk encryption is required.	For UBC-owned laptops running Windows or macOS, use the UBC IT Encryption Service. For all other laptops, use native encryption for Windows (BitLocker), macOS (FileVault) or Linux (see Section 10).
Smartphones, tablets and PDAs	Device-level encryption is required.	iOS Devices connecting to FASmail using ActiveSync are automatically encrypted; for other Devices refer to Encrypting Mobile Devices guideline.
Mobile Storage Devices/Media	Device/media-level encryption is required.	Refer to How to Encrypt USB Sticks and Other Removable Media guideline.

Stationary Devices		
Desktop computers	Full disk encryption is required for computers containing High or Very High Risk Information. Otherwise, full disk encryption is recommended.	For UBC-owned desktops, use the UBC IT Encryption Service. For all other desktop computers, use native encryption for Windows (BitLocker), macOS (FileVault) or Linux (see Section 10).
Servers located in datacentres that comply with the Physical Security of UBC Datacentres standard	No full disk encryption required; however, encryption of High or Very High Risk Information may be required depending on the circumstance.	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 • AWS Canada • Other third-party servers approved by the CISO	No full disk encryption required; however, encryption of High or Very High Risk Information may be required depending on the circumstance.	N/A
Other Servers than listed above	Full disk encryption is required.	UBC IT Encryption Service. See Section 10 for Encryption of Devices using Operating Systems other than Microsoft Windows and Apple macOS (e.g. Linux).

7. 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.
8. 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).
9. If a Device is lost or stolen, it is essential for the University to be able to accurately report on its encryption status. UBC's Encryption Service automatically reports encryption status (whenever connected to the UBC network) to validate that encryption was active at the time of loss or theft. Users who are not using UBC's Encryption Service, or an equivalent service that automatically reports status, must provide a written confirmation of the encryption status at the time of loss or theft.

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

10. 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:
    a. Option 1 – An encrypted Virtual Machine (VM);
    b. Option 2 – An encrypted partition; or
    c. Option 3 – An encrypted home directory.

11. The local IT team(s) must advise Users who implement any of the above options that:
    a. these alternative options are not as secure as full disk encryption;
    b. the User must store all Medium, High or Very High Risk Information in an encrypted area on their Device; and
    c. the User must put full disk encryption in place as soon as practically possible.

12. University IT Support Staff must also send an email to privacy.matters@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.

File-Level Encryption Requirements

13. For instructions on encrypting Word, Excel and other general files, refer to the How to Encrypt Files Using Common Applications guideline.
14. For requirements on emailing UBC Electronic Information, refer to the Transmission and Sharing of UBC Electronic Information standard.

Password Requirements

15. Strong passwords must be used for encryption in compliance with the Password and Passphrase Protection standard.
16. 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 reliable Key Escrow service, 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.

Technical Requirements

17. 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.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Cryptographic Controls standard

Password and Passphrase Protection standard

Transmission and Sharing of UBC Electronic Information standard

Encrypting Mobile Devices guideline

How to Encrypt Files Using Common Applications guideline

How to Encrypt USB Sticks and Other Removable Media guideline

Security Considerations for International Travel with Mobile Devices guideline