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 Confidential Information. This standard does not apply to Sensitive or Public Information. 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 (a type of Confidential Information) stored on a laptop or a mobile Device, which has been affirmed by the British Columbia Information and Privacy Commissioner in her 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. Wherever possible, encryption should be implemented at the Device level, as follows:

Device	Encryption Requirements for Confidential Information[1]	Recommended Encryption Toolset
Servers	Encryption is not required if server is located in a datacentre that complies with the Physical Security of UBC Datacentres standard. Otherwise, full disk encryption is recommended	UBC IT Encryption Service
Desktop computers	Full disk encryption is recommended	UBC IT Encryption Service
Laptop computers	Full disk encryption is required	UBC IT Encryption Service
Mobile Computing Devices (e.g. smartphones, tablet computers)	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 (e.g. USB keys, CDs, DVDs, tapes, portable hard drives)	Device/media-level encryption is required	Refer to How to Encrypt USB Sticks and Other Removable Media guideline

[1] Additional requirements for these types of Devices are set out in the standards on Working Remotely and Securing Computing and Mobile Storage Devices/Media

7. Using Mobile Devices to store Confidential 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 Confidential 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; to that end, Users must either:
    a. ensure that encrypted UBC-owned Devices automatically report their encryption status (whenever connected to the UBC network) to validate that encryption was active at the time of loss or theft (UBC's Encryption Service offers this functionality); or
    b. provide a written confirmation of the encryption status at the time of loss or theft.

File-Level Encryption Requirements

10. When it is not feasible to apply encryption controls at the Device level, it is recommended that any files that contain Confidential Information be encrypted.
11. For instructions on encrypting Word, Excel and other general files, refer to the How to Encrypt Files Using Common Applications guideline.
12. For requirements on emailing Confidential Information, refer to the Transmission and Sharing of UBC Electronic Information standard.

Password Requirements

13. Strong passwords must be used for encryption in compliance with the Password and Passphrase Protection standard.
14. 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. Users 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

15. 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

Securing Computing and Mobile Storage Devices/Media standard

Transmission and Sharing of UBC Electronic Information standard

Working Remotely 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