a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #16
Cryptographic Controls

Introduction

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

Cryptographic Requirements

4. Encryption usage must be risk based and must take into account the sensitivity of information as per the Encryption Requirements standard.
5. Encryption strength must be AES-128 bit or equivalent, at a minimum; AES-256 bit encryption is preferred as it provides greater protection.
6. Cryptographic hash functions must be strong: SHA256, SHA512, RipeMD-160, WHIRLPOOL or equivalent.
7. Whenever a password or passphrase is used as an encryption key ("Key"), it must follow the standards defined in the Password and Passphrase 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.
8. 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.
9. The following requirements apply to X.509 certificates:
    a. X.509 certificates used for the securing of Sensitive or Confidential Information during User transmission must be issued by a trusted third party CA, as part of a Public-Key Infrastructure (PKI);
    b. server-to-server transmissions should be encrypted and should use a trusted third party certificate;
    c. servers must be configured to use TLS version 1.0 at a minimum; TLS version 1.1 is preferred;
    d. newly purchased or renewed X.509 certificates must be a minimum of 2048-bits; and
    e. X.509 certificates may be purchased under the University's Enterprise account, via security@ubc.ca.

Full Disk Encryption (FDE)

10. In order to help Users to comply with the above requirements, the University provides a secure and effective FDE solution to protect laptop and desktop computers.

Key Management

11. 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 service is recommended for this purpose because it is reliable and secure. See the Key Escrow guideline for more information. • Alternatively, the Key may be recorded on a piece of paper and locked in a secure location such as a safe. • 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.

Additional Requirements for Merchant Systems

12. Users must not store authentication data collected in Merchant Systems after authorization (even if this data is encrypted); authentication data includes:
    a. the full contents of any track from the magnetic stripe or chip;
    b. the card-verification code or value (three or four-digit number printed on the back/front of a payment card); and
    c. the personal identifier number (PIN) or the encrypted PIN block.
13. 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.).

Related Documents

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

Encryption Requirements standard

Password and Passphrase Protection standard

Reporting Information Security Incidents standard

Key Escrow guideline