INFORMATION SECURITY GUIDELINE

Key Escrow

Introduction

1. This guideline is meant to provide assistance with key escrow, which is a method of storing keys (Passwords or Passphrases) used to encrypt and decrypt information so that they can be recovered if they are lost.
2. This guideline has been issued by the Chief Information Officer to supplement the Cryptographic Controls standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Security and Privacy of Key Escrow

3. Key escrow provides a secure and private method of recovering keys used to encrypt information.
4. Key escrow cannot be used to track the location of an individual. The only IP address that is recorded is the IP address assigned by a wireless access point, which is typically non-routable (in the 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255 or 192.168.0.0 - 192.168.255.255 ranges). These IP addresses are not unique and cannot be used to track a User's location.
5. Additionally, UBC's encryption service is only accessible on campus or via VPN, which means that UBC can only record UBC-owned IP addresses; if Users connect from off-campus via the VPN, then the system would only record the IP address assigned by UBC.

UBC's Key Escrow Service

6. The encryption packages (McAfee & PGP) that UBC IT is currently supporting, offers key escrow services. These services are automatically enabled for all users of these encryption packages.
7. After the key escrow service is enabled, Users may use it to recover keys at any time by calling the UBC IT Help Desk.

Alternatives to Key Escrow

8. The following are alternatives to key escrow:
   a. use a Password Safe (see the Password Safe guideline for more information);
   b. print out the key and lock it in a safe;
   c. save the key file to a USB drive and lock it in a safe; or
   d. if using Apple's FileVault 2, read the following article on "How to create and deploy a recovery key for FileVault 2" (http://support.apple.com/kb/ht5077).

Related Documents

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

Cryptographic Controls standard