Recovery Management Guidelines

Each of the University’s recommend disk encryption tools has mechanisms to recover data in the event that a user’s password becomes unavailable. A recovery password or key (long character string) is usually the simplest recovery mechanism. Note: Sophisticated schemes for automated key management and deployment require a central administration mechanism (such as Active Directory or Open Directory) that is not available within the University at this time.

The following are recommended recovery mechanism guidelines:

BitLocker: Generate and record the recovery password that consists of a unique 48-character numeric code, and that the user is given the option of recording during the initial encryption process.

FileVault: Generate and record the Master Password, set by the user in the System Preferences before actually enabling FileVault.

FileVault 2: Record the disk’s Recovery Key, consisting of a 24-character string that is generated during the initial FileVault 2 enablement and configuration.

TrueCrypt (Linux): Create the TrueCrypt Rescue Disk (CD/DVD) that is generated during the process of preparing the system/drive for encryption.

The following are recommended recovery password/key/disk management guidelines:

Recovery Passwords/Keys:
Where recovery passwords/keys are generated, require users to record on paper (or USB stick) the password/key, and then place the record in a sealed envelope which they will supply to their Chair, or similar authority (as declared by your department/unit), for safe keeping in a physically secured location. Secured in this instance requires a locked container inside a room with very limited and controlled access, such as a departmental safe or a filing cabinet with a strong lock in the Chair’s office. The sealed envelope requires some form of identification of the user/laptop owner (such as their CCID username).

Recovery Disks:
Where recovery disks are generated, place these in a sealed envelope supplied to the Chair, or similar authority (as declared by your department/unit), for safe keeping in a physically secured location. Secured in this instance requires a locked container inside a room with very limited and controlled access, such as a departmental safe or a filing cabinet with a strong lock in the Chair’s office. The sealed envelope requires some form of identification of the user/laptop owner (such as their CCID username).