Policy Number	9.5
Approval Body	Executive Committee
Policy Officer	Director ITS
Approval Date Revised	March 2009 December 2012

9.5 DATA BACKUP + RECOVERY

ENABLING LEGISLATION + LINKED POLICIES

Office of the Government Chief Information Officer, Province of BC:
http://www.cio.gov.bc.ca/legislation/policy/isp.pdf

OBJECTIVE

Emily Carr University of Art + Design (University) requires critical data to be periodically backed up and that backup media (which include both tape and disk drive systems) be stored in a secure manner. This policy is designed to protect data in the University to ensure it is not lost and can be recovered in the event of a disaster such as equipment failure, human error, intentional destruction of data or disaster. The policy is not designed to recover files accidently deleted by users although ITS will attempt such a recovery on a best efforts basis.

SCOPE

This policy applies to all critical data in the University. "Critical data", in this context, includes email, shared department files, online course content, specific databases, web content delivered by the main University web server, and operating systems. The definition of critical data, and scope of this backup policy, will be reviewed on an annual basis.

This policy does not apply to data that is stored in the University's Enterprise Resource Management System, which is currently Datatel's Colleague software. This system is outsourced and backup provisions are detailed in the outsourcing agreement.

This policy applies to students, faculty and staff who may be creators and/or users of such data. The policy also applies to third parties who access and use University systems and IT equipment or who create, process or store data owned by the University.

POLICY

1. Backups will be performed on a regular schedule as determined by IT Services.
2. Backups will be stored in a secure location with controlled access. Proper environmental controls (eg. humidity, temperature, fire protection) shall be maintained at that location.
3. Any exceptions to the backup policy will be fully documented.
4. Three types of backups will be performed:
   - Full backup: contains all data in folders/directories identified for backup
   - Snapshot backup: which contain real time mirrored copies of data on disk drive file servers and are available for immediate recovery

- Tape Archive backup: contains all data in folders/directories identified for backup. This backup type is for onsite archiving and offsite storage. Archive backup will only cover Emails

5. Full backups are performed weekly and will be retained for 4 weeks.
6. Archive backups are performed monthly and will be retained for 52 weeks.
7. Snapshot backups are retained for one day and are used for immediate restoration of data.
8. Email backups are performed via snapshot backup and tape archive only.
9. Backup tape media that is not in use will be recycled. Any backup tape media that cannot be reused will be destroyed in an appropriate manner. Backup tape media that is reused for any purpose other than backups will be completely erased prior to reuse.
10. Backup procedures will be periodically tested to determine if files can be restored.
11. IT Services is responsible for backing up data that is stored in central systems and databases. Data residing on individual workstation hard drives is the responsibility of the user to backup. Students, faculty, staff and third parties who store data on University equipment are responsible for ensuring the data is stored in a way that will ensure it is properly backed up.
12. IT Services will advise users on backup procedures, supported tools, and options for data stored on workstation hard drives or external peripheral devices. However, critical data should not be stored on such media.
13. All backup media will be clearly labeled and accurate records will be maintained of backups performed and to which backup media they belong.
14. Requests to retrieve or recover data from backup will be made via email to the Network Operations Coordinator in IT Services within one business day of data loss.
15. Files that fall under University or BC Ministry of Advanced Education and Labour Market Development electronic records retention policy are the responsibility of the user and department. Such files must be maintained in a retrievable format independent of backups. University backups are not intended to satisfy compliance requirements.

POLICY SUPPORTS

9.5.1 Data Backup + Recovery Procedures