IT BACKUP STANDARDS

PURPOSE

The purpose of this document is to support and outline in detail the requirements of the IT Backup Policy. These requirements are mandatory and must be adhered to by all data custodians and backup administrators.

Backup Media

Backup media include either tape, disk or cloud storage.

External hard drives and thumb drives are not considered reliable backup media and therefore must NOT be used as primary backup media.

Backup tapes must have a lifespan of no more than five (5) years. Tapes less than 5 years old will be recycled. Tapes more than 5 years old will be destroyed. Tapes no longer required will be destroyed

Backup media will be identifiable as belonging to Brock University. Tapes must be appropriately labelled with a human readable identifier as well as a machine-readable barcode.

Backup Methodology

Backups must be automated.

Backups must be performed on a scheduled basis to meet specific recovery times objectives (RTO) and recovery point objectives (RPO) parameters set by the data owners (see Backup Definitions for RTO and RPO definitions). If no specific RTO or RPO is defined, there is no guarantee that data will be recoverable.

Data Identification

It is the responsibility of the data owner to identify data that is critical and needs to be backed up. This identification is captured as requirements during the implementation cycle of a system or service. Changes to this can be made by the data owner via a support request at the Information Technology Services ("ITS") Help Desk.

	Data and files not accessible by the backup system will not be backed up.
Additional Backups	Data or system backups that are required outside of the established backup schedule can be requested via an ITS Help Desk support request.
Backup Testing	Backup schedules must be developed for all new systems and the restore must be tested prior to putting into production.
Secure Storage	At least one copy of the backup data must be stored in a location that is geographically separate from the source data. This site must be secure. Access permissions to the secure location must be reviewed annually by the Director, Infrastructure. During transport of backup media to the secure storage location, the media in transit must not be left unattended.
Destruction of media	Recycled media may be overwritten and reused. Retired media must be destroyed so it is unreadable and cannot be accessed.
Backup Inventory	An inventory of all removable backup media must be maintained by the backup administrator, with the media identified including the systems associated with the media set. A physical inventory of removable backup media must be conducted annually. Exceptions must be identified and investigated. The results must be reviewed and signed off by the Manager, IT Infrastructure.
Network Device Backup	A log of current network devices and their configurations must be maintained to aid in recovery of the devices to their most recent state if required.

Network administrators are responsible for maintenance of this log and a backup copy.

The log must be reviewed annually for completeness and accuracy, with exceptions identified and investigated by the network administrator. The results must be reviewed and signed off by the Associate Director, Infrastructure.

Backup Monitoring

The backup log must be reviewed daily during business hours (Monday - Friday) by the backup administrators to identify exceptions / failures.

In the event of a backup failure, the backup administrator must assess the failure for severity and make appropriate corrections to ensure the viability of the backup data. Integrity of backups and adherence to backup schedules should be checked periodically with the backup reports provided by the backup software.

Server Backup Software

All Brock University system and server backups must be performed using backup software that meets the standards for data backup as defined in this document. This includes Microsoft System Center Data Protection Manager (DPM) for Windows systems, EMC Networker Software for Linux systems, NetApp Snapshots, Hyper-V replication, Idera.

Database Backups

Database backups are used for data recoveries and may be used in conjunction with a system level backup. In all cases, database backups must be stored outside of the original source server.

Backup frequency will be established in consultation with the appropriate DBA.

Backup Definitions

Protection Group: A protection group is a collection of data sources that share the same protection configurations and settings.

Recovery Point Objective (RPO): The age of files that must be recovered from backup storage for normal operations to resume if a failure occurs.

Recovery Time Objective (RTO): The targeted duration of time within which a business process must be restored after a disruption to avoid unacceptable consequences.

Replica: System Center Data Protection Manager (DPM) creates a replica of the data on its own storage subsystem. This happens on a set schedule and is called a replica.

Synchronization: Synchronization is the process by which DPM transfers data changes from a system to a server and then applies the changes to the replica. It relies on synchronization to keep the replicas synchronized with live data.

Synchronization Frequency: DPM allows a synchronization frequency level interval anywhere from 15 minutes to 24 hours.