Goal of Backup Policy

The goals of this backup policy will be as follows:

- to safeguard the information assets of the Columbia College Computing Community.
- to prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster.
- to permit timely restoration of information and business processes should such events occur.
- to manage and secure backup & restoration processes and the media employed within these processes.

Backups Policies

CCIT will provide policy-based, system level, network-based backups of server systems under its stewardship.

Working with the Columbia College Computing Community and its business functions, CCIT will implement backup policies on a per system basis that define:

- **Selections:** what information is to be backed up on systems.
- **Priority:** relative importance of information for purposes of the ordering of backup jobs.
- **Type:** the frequency and amount of information to be backed up within a set of backup jobs.
- **Schedule:** the schedule to be used for backup jobs.
- **Duration:** the maximum execution time a backup job may execute prior to its adversely affecting other processes.
- **Retention Period:** the time period for which backup images created during backup jobs are to be retained.

Definition of Retention Period

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed on CCIT-maintained systems during the time period defined by system backup policies.

Backup retention periods are in contrast to retention periods for information defined by legal or business requirements.

System backups are not meant for the following purposes:

- to archive data for future reference
- to maintain a versioned history of data

Default Schedule of Backups

Unless a system supporting an application or business function requires a custom schedule, CCIT will backup systems using a default schedule of weekly full backups and subsequent differential-incremental backups prior to the next full backup.

During backups, point-in-time images of information stored in active, permanent storage (e.g. hard disks) will be copied to magnetic tape or other media over a private network or virtual private network medium.

Full backups will back up all files specified within a system's backup policy, regardless of when they were last modified or backed up. Differential-incremental backups will back up all files that have changes since the last successful incremental or full-backup.

The media containing a system's weekly full backup and full set of subsequent differential-increment backups will comprise its weekly full backup media set.

Through use of weekly full backups and subsequent differential-incremental backups, backup windows (time period required to perform backups of one or more systems) will be minimized as will be the number of media required to store the backups. This will assist in ensuring good system performance for business processes.

Restores will require a longer period of time as the last full backup and all differential-incremental backups that have occurred since the last full backup are required. However, due to the

frequency of backups, at most one week of tapes would be required in the event of a complete system failure.

Thus, this policy works to minimize the time required to backup systems (the common case) while limiting the potential time required to perform a full-system restore in the event of a system failure (the uncommon case).

CCIT will schedule backup windows for systems so as to minimize disruption to business functions and ensure accomplishment of the weekly full – daily differential-incremental policies described above.

Storage Locations and Retention Period of Backups

Unless a system supporting an application or business function requires a custom retention period, CCIT will maintain 12 weeks of full and incremental backups.

Backup tapes for the current weekly backup period will be stored within the Computer Center for purposes of current backups and restores.

Tapes representing backups from the former weekly backup period will be maintained within a secured, fireproof safe within CCIT's offices until such time as the backup images stored on these tapes expire and the tapes are re-used or destroyed.

After a successful full weekly backup, a copy of the full backup's images will be made and stored in a secure, off-site media vaulting location for the period of one month for disaster recovery purposes.

This will ensure that no more than one week of information would be lost in the event of a disaster in which campus systems and backup images are destroyed.

After the period of a month has elapsed, the tapes will be returned to CCIT and re-used or destroyed.

Backup Verification

On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

- to check for and correct errors
- to monitor duration of the backup job
- to optimize backup performance where possible

CCIT will identify problems and take corrective actions to reduce any risks associated with failed backups.

Test restores from backup tapes for each system will be performed at least every two months. Problems will be identified and corrected. This will work to ensure that both the tapes and the backup procedures work properly.

CCIT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

Systems Management

CCIT will ensure on an on-going basis that all elements of its backup system are documented and maintained in such a manner as to ensure:

- the integrity and confidentiality of data copied during backup and restore operations
- appropriate access to data maintained within the backup system
- recoverability in the face of system failure or disaster
- optimal performance
- stability

Elements of the backup system requiring ongoing systems management include, but are not limited to:

- client software
- hardware drivers
- server software
- network connectivity & communications
- storage devices (e.g. tape library)

Media Management

Media will be clearly labeled and logs will be maintained identifying the location and content of backup media.

Backup images on assigned media will be tracked throughout the retention period defined for each image. When all images on the backup media have expired, the media will be re-incorporated amongst unassigned (available) media until re-used.

Periodically and according to the recommended lifetime defined for the backup media utilized, CCIT will retire & dispose of media so as to avoid media failures.

Storage, Access, and Security

All backup media must be stored in a secure area that is accessible only to designated CCIT staff or employees of the contracted secure off-site media vaulting vendor used by CCIT.

Backup media will be stored in a physically secured, fireproof safe when not in use.

During transport or changes of media, media will not be left unattended.

Retirement and Disposal of Media

Prior to retirement and disposal, CCIT will ensure the following:

- the media no longer contains active backup images or that any active backup images have been copied to other media
- the media's current or former contents can not be read or recovered by an unauthorized party

With all backup media, CCIT will ensure the physical destruction of the media prior to disposal.

Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made through processes defined within CCIT's Technical Support Policy.

As the restoration of information has security consequences including:

- possible escalation of privileges by parties authorized to access information
- access by non-authorized parties

CCIT will carefully verify that the request for restoration of information is authorized by the owners of the information prior to performing the restoration.

CCIT will additionally ensure that the information restored is restored to a file system location with access controls appropriate to the information being restored.

Degradation of Service

Should a failure or defect of the backup system threaten the recoverability of a computing system or its information, CCIT will take immediate actions to correct the situation.

Additionally, CCIT will attempt to warn all users and owners of applications & information of the failure or defect and the potential scope of information loss.

CCIT will work with those warned to mitigate potential or actual risks until such time as full-service can be restored.

Disaster Recovery Considerations

As soon as is practical and safe post-disaster, CCIT will:

- Restore existing systems to working order or obtain comparable systems in support of defined business processes and application software.
- Restore the backup system according to documented configuration so as to restore server systems.
- Obtain all necessary backup media to restore server computing systems
- Restore server computing systems according to the priority of systems and processes as outlined for restoration and recovery by:
    1. Columbia College's Disaster Recovery Plan, or
    2. the point-in-time direction of Columbia College's senior management