Computer/Server Backup Policy

COE–CSB–01

1.0 Purpose
To provide College faculty and staff with an overview of backup services offered by Electronic and Computer Services (ECS). Backup services provide for recovery of files that may have been accidentally erased or for disaster recovery in the event of a system or disc failure. Furthermore, departments and individuals are strongly encouraged to adopt their own system backup policies and procedures. Short of having departmental or personal system backup services, individual may purchase these services from the University’s Information Technology Services (ITS); the fees for ITS backup services are annual charges that are based on the amount of required storage space.

2.0 Scope
The College’s primary servers, Dean’s Office servers, and some twenty departmental and organizational servers managed by ECS are backed-up nightly. Faculty and staff files stored on departmental servers are included in the nightly backups.

3.0 Policy
The College of Engineering’s backup services are limited to core College and departmental servers. These servers are backed-up according to a cyclical schedule according to the following procedures:

- Faculty and staff are encouraged to store critical proposals, documentation, or administrative files on their departmental servers.
- Access to servers is through a College of Engineering account that may be exhausted by a member of the ECS Support Group (support@engr.psu.edu) or may be established through a College of Engineering Departmental Technical Contact.
- Complete server backups are completed once a month.
- Differential or Incremental backups are performed nightly. Monthly backups are retained for a minimum period of two (2) months; files accidentally or purposely deleted longer than the retention period are permanently lost and not recoverable.

ECS managed College Email and Virtual Server environments and backup operations thereof:

- Both the College email systems and the virtual servers operate in a dual redundant mode.
  - The email servers operate in tandem to one another with one system acting as the primary email server and the second as a mirrored "hot" server. Data on the primary email server is dynamically and continually replicated on the secondary server; should the primary system fail, services can be automatically switched over to the secondary system with little or no loss in business continuity.
  - The College virtual server environment consists of dual systems which have a local data storage and a secondary storage bank of equal size to store replicated data from the other server farm. Data from one virtual server network is automatically replicated to the secondary storage bank of the other Virtual network at regular intervals. The two Virtual server farm share the LUN load within the College, each containing half the total operational load. The LUNs of one Virtual network also reside on the other but are not functioning in an operational mode. This mode of operation form a disaster tolerant pair of Virtual server farms because each pair is physically separated and on a separate University backbone connection. Should one of the Virtual server farms fail or loose backbone connectivity, its non-operation LUNs stored on the other Virtual network farm can be activate to access the replicated storage back to provide for business continuity.
• The services of both Email and Virtual network systems are under controlled access and are available only to authorized users. Access is through a College of Engineering account that may be established by a member of the ECS Support Group (support@engr.psu.edu) or may be established through a College of Engineering Departmental Technical Contact.

The backup philosophy relating to other than ECS managed servers is as follows:

• Faculty and staff are strongly encouraged to develop a backup strategy for their desktop and/or laptop computers.
• Faculty and staff have the option of purchasing backup space from ITS.
• Faculty and staff have the option of procuring disk drive or tape backup systems that they or their departmental Technical Contacts may manage.
• All backup solutions must meet University and College Disaster Recovery requirements and so must be physically isolated from the hosts they serve. This is necessary to prevent data loss in the event of a catastrophe whereby an entire facility is lost.

Security requirements for data backup

• Data backups must meet the same technical and physical security requirements as for the “at rest” storage on the hosts they serve. For example, a backup solution that serves hosts containing Public, Internal/Controlled, and Restricted data must meet the same security requirements as the highest security client it serves (i.e., Restricted) as set forth in the University and College Data Classification Standards and Security Requirements policies.

4.0 Enforcement

ECS personnel will ensure that all College critical servers and departmental server managed by ECS are backed-up according to this policy.

5.0 Revision History

Last updated: 11/17/10