Compliance Procedure

Title: **System Backups and Restoration (Non- Db) Procedure**
Reference Number: **3.4.2.2**

Purpose

The purpose of this compliance procedure is to define the methods in place to ensure that proper backups are done for Non Db hardware servers. Such servers are those containing data for various campus applications and customers versus those in place for global usage relating to Banner processes.

Additionally, this procedure identifies the process by which data files (Non Db) are restored to the network drives for customers.

OCCS does disc and tape backups for disaster recovery purposes versus data retention purposes. Data owners and users should insure file management practices comply with required retention policies.

Procedures & Related Information

Backups:

OCCS will utilize enterprise software (disc and tape management) to execute backups of the various servers within the data center. The current product used to perform this task is Tivoli Storage Manager (TSM).

The time of day for execution of backups shall not be limited to the non prime hours. Server Support staff and the System Owner shall determine the interval window in which the backup shall occur.

Backup schedule and the backup interval used shall be determined as part of the product life cycle at implementation stage of a particular server by the Server Support Group and System Owner. As a server is put into production, the backup cycle shall be determined, implemented, and tested. Such backups and selection of the backup window shall be signed off as being acceptable to the Server Support group and System Owner after which such information will be relayed to Data Center Operations for inclusion in the Backup Schedule for management and monitoring.

Server backups execute automatically at predetermined times without intervention by staff, other than operations removing full tapes or adding additional scratch tapes, and a daily assessment of proper completion.

Operations will perform a daily assessment of the proper completion of backups. Successful completion and/or failure of a specific server shall be posted as entries in the activity log viewed by Operations staff and Server Support group. All failures will be sent out as notifications to insure they are brought to the attention of proper support teams.

Backups for all operating systems disks (Windows, Linux or Solaris etc) are represented by one (1) active version, one (1) inactive version plus one (1) deleted version. The inactive version is maintained for thirty (30) days while the deleted version is maintained on the system for sixty (60) days before being permanently removed.

For UNIX file systems outside the firewall, which includes applications and user data, backups are represented by one (1) active version and four (4) inactive versions plus one (1) deleted version of files. The inactive versions are maintained for thirty (60) days while the deleted version is maintained on the system for sixty (30) days before being permanently removed.

For Microsoft file systems outside the firewall, which includes applications and user data, backups are represented by one (1) active version and four (4) inactive versions plus one (1) deleted version of files. The inactive versions are maintained for sixty (60) days while the deleted version is maintained on the system for thirty (30) days before being permanently removed.

University Exchange Email files for faculty and staff email is managed in accordance with the Email Archive & Retention Standard (Standard #01.7). Users should not confuse file retention periods with email retention periods as these are not equivalent. Files are represented one (1) active version and one (1) inactive version plus one (1) deleted version of all files The inactive version is retained indefinitely until replaced on the system while the deleted version is retained for thirty (30) days after the file is deleted.

There may be very specific data cases where deviations from these standards are required for legal, historical or security reasons. Each specific case must be individually documented and approved by the Systems Support group and Data Owner and registered with the Data Center staff to insure proper monitoring and management of the backups.

A full list of servers being backed up (non Db) by name along with their scheduled starting times is maintained in the Data Center Operations area.

Restorations:

This process is specifically for Non Db files and is normally utilized by customers.

The Server Support Group is the primary staff with the responsibility of restoring files for customers.

The method of restoring data files consists of utilizing the Tivoli Storage Management system, which tracks where particular files are located and automatically accesses disc pools or requests the proper tapes to be mounted and seeks to restore a requested file.

The tool made available to customers for file restoration is an email list serve called “Data Restore”.

Restoration of data from directories owned by users that no longer work at or have left the University must be generated by the Budget Unit Director for that position. For these cases, the request for data restoration must be coordinated through and approved by the OCCS Security staff.

Information on the use of “Data Restore” can be found on the OCCS web site at http://occs.odu.edu/support/datarestore/backup.shtml.

In general, users can request files be restored by sending an email to datarestore@odu.edu. The email should contain the name and location of the file to be restored to the system. It should also contain the date of the last known version that had good copy.

Once the request is received within OCCS, Server Support staff will make very attempt to locate the file being referenced. If there are any questions concerning the file, date, location etc, they will contact the customer directly for additional information and clarification. The Server Support group will notify the customer when the file is restored and where it is located for them to access it or if the request cannot be fulfilled.

Definitions

Active Version is the term referring to the backup copy of the most recently modified version of a file.

Deleted Version is the term referring to the last remaining copy of a file that has been backed up after the file has been completely deleted from the system it was on.

Inactive Version is the term referring to all previously modified copies of files that are not the most recent modification that are retained on the backup system.

Linux is a term referring to all forms of the Linux operating system whether they are open source or commercially sold. These can include, but are not limited to Red Hat, CentOS, SUSe and any others currently available and run in the data center.

Non-Db is the term used to reference any file that is not directly related to a managed known database system. The database systems recognized centrally on the campus can include database files from Oracle, SQL, MySQL or other enterprise databases. MS Access is typically not considered in this class.

OCCS is the acronym for the official name of the Office of Computing and Communications Services.

Solaris is the term used to reference all forms and derivatives of the Solaris operating system provided by Sun Microsystems/Oracle or from open source.

Tivoli Storage Manager (TSM) is an Enterprise class backup system sold by IBM. TSM typically backs up all files in an “incremental forever” format. This means that it backs up the entire system the first time and every time after that it only backs up files that have changed since the first backup.

Windows is a term to reference all Microsoft versions of the server operating system. These can include but are not limited to Windows 2000 Standard, Windows 2003 Standard, Windows 2003 Enterprise, Windows 2008 and any other variations active in the data center.

Policy References **ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.**	
Ⓟ Policy Foundation:	Federal and State Law Policy 3507 Operations Management
🗗 Related Standards:	IT System and Data Backup and Restoration Standard Server Management Standard Network Management Standard Change Management Standard Print Management Standard Physical Security Standard
🗀 Related Procedures, Forms:	System Monitoring procedure Console Logging Procedure Customer Notification Procedures Alert Posting Procedure
ⓘ Related Guidelines:	System Monitoring Tips Call Out List Customer Contact List
🛠 Maintenance:	Office of Computing and Communications Services
✔ Effective Date:	Reviewed on an annual basis
✔ Approved by:	Rusty Waterfield Acting Assistant Vice President, Office of Computing and Communications Services
✔ Approved:	University Advisory Council on Technology ☒ Required for Standard