Computer Systems Backup Policy
Information Services
University of Richmond

The University of Richmond requires that centralized computer systems maintained by Information Services fall under one of several backup profiles as described below. The purpose of a systems backup is to provide a means to restore the integrity of a computer system in the event of a hardware/software failure, physical disaster, or human error.

A system backup consists of either a full backup, incremental backup, or a combination of the two. A full backup is performed when a system is "offline" and contains every file on the system whereas an incremental backup is typically performed while a system is running and includes only those files that have changed since the last full backup. System backups are performed on a periodic schedule as determined by business or application owners in conjunction with Information Services.

System backups are typically stored on both disk and tape media. Once the backup retention period expires, the disk and tape media is either re-used (over-written), erased, or destroyed in an approved manner.
System backups consist of two copies. The first copy is stored on a disk pool located in the data center. The second copy is stored on tapes that are sent off-site on a weekly basis. Both copies have the same retention settings, which are specified in the System Backup Profiles section below. All tapes are encrypted.

IMPORTANT: Backups save a copy of data, files, and directories found on the disk at the point in time the backup was performed, but do not record all activities or contents of users' files throughout the day. As a result, it is completely possible for a user to create and delete a file during the course of a day which will never appear on a backup. It is also important to note that a system backup is not intended to serve as an archival copy or to meet records retention requirements—these needs are dictated by business policies and typically require dedicated hardware/software solutions.

<u>System Backup Profiles</u>

1. **Standard Backup** – The standard backup provided for most centralized University computer systems (applications, databases, e-mail, netfiles, etc) is as follows:
    a. A full system backup is performed weekly on a day and time agreed upon by the business or application owner and is retained for two weeks. The one exception to this is Exchange e-mail, for which backups are retained for 30 days.
    b. An incremental backup is performed daily (between full backups) and is also retained for two weeks.

2. **Critical System Backup** – Certain enterprise-wide systems are deemed critical to University operations and dictate longer retention periods. Systems that fall into this

category include Banner, Blackboard, and some library systems. The backup schedule for these systems is as follows:

a. For administrative systems (e.g., Banner), a full system backup is performed weekly and retained for one month. The last full backup of each month is retained for 13 months.
b. For academic systems (e.g., Blackboard and Library), a full system backup is performed weekly and retained for two weeks. The last full backup of each semester is retained for 13 months.
c. Prior to a major upgrade of a production system, database, or application, a full system backup is performed and retained for 13 months.
d. An incremental backup is performed daily (between full backups) and is retained for two weeks.

3. **Special Request Backup** – Some departments or applications may require an exception to the standard backup retention periods mentioned above. Exceptions are permitted, but must be fully documented and any associated costs may need to be justified and/or reimbursed by the requesting department or application owner.

4. **No Backup** – If a system does not fall under any of the backup profiles listed above, it may not be backed up. If this is cause for concern or you would like to confirm whether or not a particular system is backed up, please contact Information Services. Systems that fall under this category might include development or test systems that do not contain important business or academic data. However, most systems that are centrally managed by Information Services are backed up on one of the schedules listed above.

For information about backing up your personal computer or personal data, please see the Help Desk's web page on "Backups": http://is.richmond.edu/helpdesk/backups.htm

Restores of System or Data Backups

Backups are typically restored on a per request basis to recover data or files that may have been lost. However, Information Services periodically tests restores of critical system backups to ensure that backups are working as expected. In particular, Information Services tests and confirms restores of Banner financial system backups on a semi-annual basis.

Revision History

Version	Date Revised	Author	Comments
1.0	Feb 28, 2008	Troy Boroughs	Initial policy created
2.0	May 10, 2010	Troy Boroughs	Policy reviewed to include audit requirements for testing restores of Banner financial systems.
3.0	April 25, 2014	Clovis Khoury	Updated paragraphs on tapes to include tape encryption and disk pools.