Overview

Purpose

All electronic information considered of institutional value should be copied onto secure storage media on a regular basis (i.e., backed up), for disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs, identified through technical risk analysis that exceeds these requirements, should be accommodated on an individual basis.

Scope

Data custodians are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. Backup provisions allow business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of institutional data backups need to be maintained.

Definitions

University Critical Data: Data that if it were deemed unavailable to the University will have an immediate (within 24 hours) critical impact on the University.

Data Owners: Department managers, members of the top management team, or their delegates who bear responsibility for the acquisition, development, and maintenance of production applications that process SDCC information. See the Information Security Roles and Responsibilities for more information.

Data Custodians: Have physical or logical possession of either SDCC information or information that has been entrusted to the college. Custodians are responsible for safeguarding the information and making backups so that critical information is not lost.

Standard Detail

Backup and Recovery processes commensurate with legislative and business requirements must be developed, maintained, and regularly tested to ensure continued business operation and access to data and information within the required timeframe, should a risk event occur.

Backup requirements will be determined by a business risk assessment completed by the owner, and is dependent on the:

- Importance of the data and information to the function of the college.
- Acceptable transaction loss (business areas must determine what level of potential transaction loss would not be acceptable or would be too difficult to recover. This can be determined in terms of a timeframe, the number of transactions, or the amount of effort and time required re-entering data.
- The maximum acceptable outage of the system while performing backups.
- The maximum acceptable outage of system while recovering data.

In addition to regular backup processes, backups will be performed before and after major technical or business-related changes to a system or application.

An audit trail of all backup activities must be maintained.

Documentation

For all departmental information assets, documented procedures must exist for the backup and recovery processes and these documents must be readily accessible. Backup and recovery operations and the specified period of maximum acceptable outage must be documented for all systems.

At a minimum documentation must contain:

- A description of the system to be backed up;
- The individual or group responsible for ensuring that the backup and recovery occurs;
- Backup and recovery requirements;
- Backup media storage locations, including off-site storage;
- Required backup frequency e.g., daily, weekly;
- Backup cycles required;
- Backup retention period;
- Testing process;
- Recovery schedule and plan; and
- Locations of relevant software and licenses.

Backup media

Backups must be regularly tested as determined by a risk assessment or at a minimum on an annual basis to ensure data can be restored in case of a catastrophic event.

Protection mechanisms and access controls for backup media must be commensurate with the security requirements and criticality of the information stored in the backup.

Backup media must be stored and transported in an appropriate, safe, and secure manner and access to backup media must be restricted to only authorized personnel.

Off-site Storage

Based on backup requirements and backup cycles, at least one instance of a backup within a cycle must be stored off-site (physically separate from the data or system being backed up) or geographically separate, as determined by a risk assessment.

Backup media stored off site must be stored in a secure location with environmental controls (if available) and appropriate access controls commensurate with the security requirements and criticality of the information stored in the backup.

Back-up tapes will be stored off-site on a basis that is determined by the risk assessment.

Backup Media Disposal

Obsolete backup media must be disposed of in a safe and secure manner, in accordance with SDCC standard. Backup media to be disposed of must be rendered unreadable through an appropriate means and an audit trail of disposal of backup media must be maintained.