Procedure

Information Technology Data Security

Backup and Disaster Recovery Guidelines Procedures

Number:

Office of Primary Responsibility: Office of IT

Effective Date: 2021

Purpose: The goals of the backup and disaster policy are:

- To safeguard the information assets of the Rust 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 and restoration processes and the media employed within these processes

Policy:

Rust College OIT recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a daily basis.

Procedure: Server Backup

Rust College OIT will provide policy-based, system-level, network-based backups of server systems under its stewardship. 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 changed since the last successful incremental or full

backup. 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. Backup logs are reviewed daily during the week to monitor backups and correct any errors. Backups are tested periodically to verify data integrity.

Systems management

Rust College OIT will ensure on an ongoing basis that all elements of its backup system are maintained to ensure:

- The integrity and confidentiality of data copied during backup and restoration operations
- Appropriate access to data maintained within the backup system—recoverability in the face of system failure, or disaster
- The data is backed up locally to a device called DATTO; the data is stored on the device both locally and transferred to two bicoastal U.S. offsite data centers, offering protection from natural disasters and illegal access