Approved by PC 12/2022

Ferrum College Data Backup and Recovery Policy

The Ferrum College Data Backup & Recovery Policy is implemented and managed by the Information Services staff, reviewed by the Information Services Advisory Committee (ISAC), and approved by the Ferrum College President's Cabinet (PC). This policy can be modified and approved on an as-needed basis.

General

The purpose of this policy is to establish standards to ensure appropriate management of Ferrum College data. The purpose of creating backups is to provide for disaster recovery of crucial server and local workstation data. Backups also provide the ability to recover files in the event they are inadvertently deleted, corrupted, or otherwise changed in such a way that data is lost.

This policy shall apply to the following members of the Ferrum College community: faculty, administrative officials and staff who use, or access, , locally or remotely, Ferrum College's internet resources, whether individually controlled, shared, stand-alone, or networked.

Frequency

Although Information Services personnel assist in the creation of backup processes and end-user training, data backups to the designated backup server are managed by the end-user. It is the sole responsibility of the end-user community to back up their local workstation data to the backup server, and to verify that each backup job completed successfully. Date and Time stamps should be confirmed. Servers that are under Network Services control are backed up to other server disk storage areas, as necessary (determined by the Director of Network Services and Security).

Retention

How long do we keep the Data Backups for faculty, administrative officials and staff?

- Management of the backup folders and data copied to the Faculty server is the sole responsibility of the faculty/staff member or administrative official as long as they are employed by the College.
- If an employee leaves the College for reasons including but not limited to, voluntary resignation, position change within the college campus, involuntary termination, retirement or death, the data folder backups on the backup server will be retained after the status change or termination date. Administrative computing and the employee supervisor will receive an email from Human Resources about the status change or termination of employment. Once this email is received within our Administrative Computing office, an email will be sent to the IS Staff Support or IS Academic / Faculty Support person, to notify them for retention of this data in compliance with applicable law. It is the sole responsibility of the employee's supervisor to notify the Administrative Computing Office and IS Staff Support / Academic Faculty Support person in writing (email is acceptable) if special data management will be needed, and ultimately whether the data should be retained, removed, or transferred to a new owner.
- Until otherwise directed, the data will remain archived until its applicable legal retention period expires.

- All Records pertaining to ongoing or pending audits or lawsuits (including reasonably anticipated claims or lawsuits) will not be destroyed, damaged, or altered, even if the records retention period has expired, until the matter has been resolved.

Backup methods
End users will save all local workstation data to the backup server either manually or by script automation. The frequency of backups must be appropriate to the type and critical nature of the data being backed up.

Restore methods
Regular restores of data should be performed for verification of recoverability of backed-up data. This is the sole responsibility of the end-user for a local workstation. Assistance may be provided upon request.