SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **DATA RECOVERY**	Procedure 8.25.01

I. PROCEDURE STATEMENT

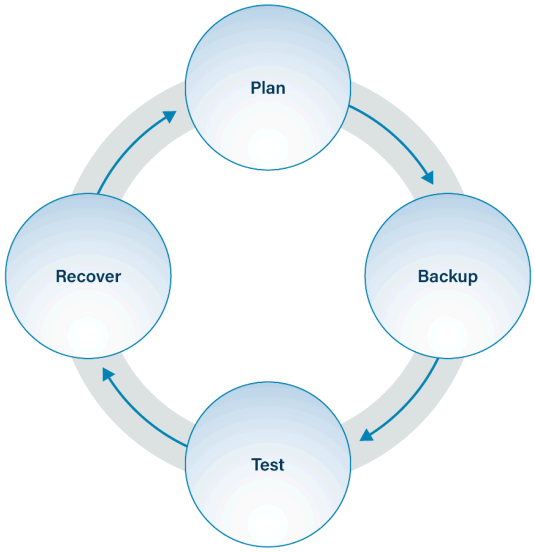
Proper planning will help an enterprise recover from different types of cybersecurity events or natural disasters in a timely manner. This *Data Recovery Procedure* provides an overarching strategy for governing the backup and recovery of data within the enterprise. This includes creating a detailed data recovery process to ensure data is backed up on the correct assets. This process should be documented and be quickly available in case an incident occurs. Additionally, procedures for securely protecting data from unauthorized access or modification alongside appropriate methods for how users should handle their data during their day-to-day work activities.

II. RESPONSIBILITY

This policy is applicable to all users and IT assets. Specifically,

- The IT Division is responsible for a majority of data recovery functions.
- Users are responsible for ensuring their enterprise data is appropriately backed up in accordance with enterprise requirements.

III. DATA RECOVERY LIFECYCLE



- **Plan –** Create a detailed course of action to handle an overall backup strategy.
- **Backup –** Take backups from enterprise assets and transfer them to other data storage locations.
- **Test –** Ensure that the backup strategy is functioning as planned. This includes ensuring that the intended data is appropriately stored and is recoverable within the timeframes established by the data recovery plan.

  Recover – Execute the plan for recovery plan and get the right data back into the hands of the enterprise. Also feeds back into the planning phase.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **DATA RECOVERY**	Procedure 8.25.01

IV. PLAN

One of the primary aspects of recovery planning is understanding what your recovery objectives are. Essentially, what data and enterprise assets are most important to your enterprise's mission and how quickly does your enterprise need systems and their data at operational status. Meeting large, complex, and quick continuity objectives will likely require much planning and resources to meet. Data owners outlined in the *Data Management Policy* 8.20 must be consulted to understand any impacts on data recovery. The *Enterprise Asset Inventory 8.18* and *Data Management Policy* 8.20 can be used to help guide these prioritization discussions, since these two inventories will contain what data is already labeled most sensitive to an enterprise's success and what assets that data resides on. These assets and data should be plainly laid out in the data recovery plan and should include backups for data stored in third-party service provider infrastructure, such as cloud platforms. Cloud service providers (CSPs) often stipulate that they do not own or are responsible for the data housed on their platforms, meaning that if the data is lost; it may be lost indefinitely. It is best to double-check with the CSP prior to onboarding to ensure that this is in-line with the enterprise's policies.

Data recovery planning should also include the types of data storage to be used for backup purposes, where that data will geographically reside once backed up, and necessary security controls to be applied to that data to protect it from unauthorized access. Cloud storage for data backups is an adequate solution, but enterprises should verify that the data is actually stored elsewhere. Even if cloud storage is used as a primary backup strategy, there needs to be a plan for network isolated, offsite backups. The reason for this is twofold: 1) preventing ransomware that enters the network from encrypting backups and 2) preventing fires or other natural disasters from destroying backups.

V. BACKUP

This part of the data recovery lifecycle includes taking data from enterprise assets and storing this data elsewhere. A backup is a duplicate of a computer system's data, but different types and degrees of backups exist. A backup is commonly viewed as a small collection of a system's overall data. Often only a few important folders are backed up, such as containing photos, receipts, contracts, or tax information. This data may be stored on another computer system, external hard drive, removable media, or cloud service. This strategy is insufficient for protecting an enterprise. Instead, a complete system image is a snapshot of all data and settings on a system, is preferred. Flavors of backups include incremental, differential, or complete.

If a system is breached by an attacker, infected with malware, or involved in an accident (e.g., fire, flood), it often takes a long time to bring a system or network back online. This could include reinstalling and reconfiguring all the enterprise systems and applications. Complete system backups rectify this issue by backing up not just important folders, but by backing up the entire computer, which can be pushed to new systems. Although this approach is a more complex solution, it makes recovery from a disaster or computer incident significantly faster. Backups protect against many malware types including ransomware and destructive malware. Using tools and service to perform automated backups is now commonplace and is an activity worth the time to setup and manage.

Lacking specific guidance to dictate the length of retention of data from production system, enterprise data can become cumbersome to manage, which may lead to accidental data loss or mismanagement. This is in part due to data being stored essentially everywhere nowadays including within the enterprise, outside the enterprise, and with third-party service providers. Additionally, removal of sensitive data no longer being used lessens the impact of a data breach since less data will be available to be stolen on enterprise assets. Data retention schedules within the *Data Management Procedure 8.20.01* should also consider the data contained within backups, as this data may not need to be saved and archived for an ill-defined amount of time. Enterprises should work to understand the relevant laws regarding data retention and their enterprise, such as the General Data Protection Regulation (GDPR). This is especially so if they are housing data that is covered by special legislation, such as medical data. Certain laws may specify timeframes that enterprises must keep data safe or mandate specific methods of destruction.

VI. TEST

The anti-malware tools on enterprise assets should be configured to warn users that a threat has been detected. These tools should also be generating logs that IT can use to research the actual sequence of events that made the anti-malware suite report an infection alert. Logs can also be beneficial when there is a single system performing analysis of all logs in an enterprise such as a Security Information and Event Management (SIEM). Some enterprises may choose to disconnect an infected system from the network and revoke its access to enterprise data while there is malware actively on an asset. It is common for IT to want to upload a malicious application to a malware tool such as Virus Total. These sites and tools can provide valuable threat intelligence about malware, but may have some drawbacks that require additional research on IT's behalf.

Additionally, users should be trained for signs of malware on their system, and what to do if the anti-malware software installed on their enterprise asset identifies a malware infection. This can be accomplished via the Security Awareness and Skills Training offered by the enterprise, codified in the College's *Security Awareness Training 8.09 Policy* . Additionally, the anti-malware tools should be configured to warn users that a threat has been detected. Note that it's never advised to shutdown or restart a computer that is infected with malware, as IT may need to analyze the system, and shutdown or restarts will either remove or partially destroy all volatile memory. It is recommended for enterprises to disconnect an infected system from the network and revoke its access to enterprise data while there is an active malware infection on an asset.

VII. RECOVER

As part of data recovery planning, enterprises should ensure that lines of communication exist between individuals charged with recovery activities and leadership roles. Additionally, granular milestones for data recovery objectives should be created to help show progress and divide recovery activities into more manageable chunks. Once an incident occurs that necessitates recovery, the data recovery plan should be put into action and implemented just as it was tested and validated. The data recovery team

should work to improve the data recovery plan after an incident in order to continuously better the plan. Data recovery teams should proceed with caution when leveraging data that was touched by malicious attackers. This data may have been subtly modified or "poisoned" in some way. It may be best to recover from data untouched by attackers. Recovery planning and communication should be considered as part of the *Incident Response Policy*.

LEGAL REFERENCES:

- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, Control 11 (Data Recovery)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

Adopted: September 2025

Revised: N/A