19-451 Data Backup Procedures and Guidelines

(A) The supporting data backup procedures and guidelines are designed to provide North Central State College with a documented and formalized Data Backup and Recovery procedure that is always to be adhered to and utilized throughout the college. Compliance with stated policy and supporting procedures helps ensure the safety and security of North Central State College's I.T. system resources and all supporting assets. Backups are a critical process for North Central State College, especially considering today's growing regulatory compliance mandates and the ever-increasing cybersecurity threats for which higher education institutions face daily. A well thought out efficient and reliable backup and data recovery is a must for ensuring the confidentiality, integrity, and availability of critical data.

(B) Data backup procedures and guidelines are designed to ensure organizational data is backed up on-site and in an off-site location and can be easily found and recovered in the event of an equipment failure, intentional destruction of data, or disaster. The Technology Services team will be responsible for all aspects of backing up servers supported by the college. Test servers will not be backed up unless requested by the server owner. Data backups will include daily incremental, and full weekly backups. The Technology Services team will also be responsible for finding and restoring data when requested or required for Disaster recovery purposes.

(C) Backup frequency is critical to successful data recovery. Technology Services has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident while avoiding an undue burden on the users, the college network, and network administrator.

(1) Full – A complete backup of data.

(a) It is the most comprehensive and complete backup of all critical data.

(b) A full backup of data will be performed once a week.

(2) Incremental – An incremental backup essentially backs-up all the files or parts of files that have changed since the previous backups were conducted regardless of the type of backup (Full, or Incremental). An incremental backup will be performed daily.

(D) Any exceptions to the types of backups and the default backup schedule are to be approved by authorized IT personnel, with a valid and justified reason. Additionally, such exceptions which are changes to the backup process are to be submitted via the IT service desk so a service ticket can be created with the formal change request. The formal request is to be reviewed by authorized IT personnel. Changes to any of the tools and utilities used for the backup process also require the use of a documented change request, initiated by select IT personnel only. The backup platform is a critical component of North Central State College's information technology infrastructure, thus great care and due diligence must be enacted when involving changes to the data backup process.

(E) Backup reporting activities, for all types of backups (Full and Incremental), are to be monitored regularly for ensuring the success of the backup process. All backup processes are to generate reporting metrics for which IT personnel are to review promptly. Such reporting metrics include, but are not limited to, the following:

(1) Confirming the current status and final result (success or failure) of all data backup processes (email, logical drives, virtual machines, etc.)

(2) Reports generated confirming the current status and final results (success or failure) of all individual backup processes.

(3) Successful backups are to be recorded as such and backup failures and exceptions are to be handled immediately, with appropriate steps undertaken for ensuring the timely backup of such data.

(4) Failures and exceptions are to be delivered via email reports from the backup utilities notifying authorized IT personnel of such issues. Depending on the nature, severity, and urgency of the backup itself and the resolution for correcting the issue, a thorough analysis is to be undertaken for correcting the issue promptly and for helping mitigate the issue in the future.

(F) Appropriate security measures are to be implemented for backups, which include all necessary physical security controls, such as those related to the safety and security of the actual backup media, server, and storage area network (SAN) device. Appropriate security requires the use of a data center or other designated main data facility that is always secured and monitored and whereby only authorized personnel have physical access to the network devices performing backups. Thus, “secured” and “monitored” implies that the facility has in place the following physical security and environmental security controls:

(1) A facility constructed in a manner allowing for adequate protection of backups

(2) Security alarms that are active during non-business hours with alarm notifications being emailed to authorized IT personnel.

(3) Access control mechanisms consisting of traditional lock and key, and or electronic access control systems, such as badge readers and biometric recognition. Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are to be retained for a minimum of 30 days.

(4) Appropriate emergency power protection is to be provided to ensure continued, balance load of power to the facility where backups reside.

(G) The data restoration procedures must be tested and documented. The network administrator is responsible for the restoration, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration.

(H) If any data retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of encryption keys. Encryption keys must be retained for as long as the data that the keys decrypt is retained.

Effective: October 28, 2020
Expires: February 1, 2026
Review Dates: 10/28/20, 2/23/21