Effective: 01-01-2009
Last Revised: 08-24-2017

Individuals having elevated access privileges (e.g. system administrators) are prohibited from accessing information they otherwise would not have a need to know, unless required to do so in the performance of specific tasks to support critical system needs. All such access must be logged and periodically reviewed. Enforcement of this standard requires sufficient resources to carefully monitor system logs. Additionally, requirements such as FERPA and State of Nebraska LB 876, policies for information dissemination and authorization, must be taken into account.

Privilege Assignment

Formal standards and procedures cover all stages in the lifecycle of user access, from the initial registration of new users to the final termination of users who no longer require access to information systems and services. The allocation of privileged access rights, which allow users to override system controls, are audited and documented. As per UNO practices, accounts may exist for a period of one (1) year, but access privileges are removed as described in Appendix A: Employee Separation Procedures and Guidelines in the event of a change in role or status with the university.

Access control privileges for university information resources shall be assigned to users via roles,

- Users must lock systems that their account is logged into before they leave the system for extended periods of time. All systems should have an auto-lock feature enabled after a maximum of ten (10) minutes of inactivity.
- Users must not reveal their authentication credentials, including passwords, to others. Control over the use of those privileges relies upon the exclusive utilization of the user account by the authorized user.
- Users must be vigilant both in recognizing and reporting security violations related to authentication credentials. All potential security violations are to be reported as defined in the UNO Digital Security Incident Response Policy.

Systems and Application Process

System Requirements

Security controls at the operating system, database, and application levels must be used to restrict access to computer resources. At a minimum the security controls must be capable of and configured to perform the following:

- Identify and verify the identity, and if necessary the IP or location of each authorized user
- Record successful and failed system accesses
- Provide appropriate means for authentication
- If a password management system is used, it must ensure quality passwords
- Where appropriate, restrict the connection times of users

Session Timeouts

thorized user

All university-owned equipment is subject to audit for unauthorized storage of regulated data. Devices authorized to store regulated data are subject to audits as deemed necessary by the Information Security Office. Reasonable prior notification of an audit will be provided. Audit results are handled confidentially by Information Security staff and reported to the Executive Regulated Data Authorization Committee in aggregate.

Training

Training on technical requirements will be provided at the time authorization is granted to electronically store regulated data by Information Services. Training must be completed before storage begins.

Policy Enforcement

This policy is enforced by the Executive Regulated Data Authorization Committee. Failure to comply

Director of Human Resources (HR): Responsible for the notification and facilitation of employee separations.

Administrative De2Pt8q43.gtions.

This policy covers the following sections of PCI-DSS 3.2:

8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
8.2 Ensure proper user-authentication management for non-consumer users and administrators on all system components.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods.
10.1 Implement audit trails to link all access to system components to each individual user.

This policy addresses the following sections of the UNO Security Manual: Chapter 13: Access Control

History

This policy is an update to the Systems Access Policy that was previously updated in 2014.

Policy revision on August 24, 2017 to modify the procedure for retiring staff employees.
