UNIVERSITY OF NEBRASKA AT OMAHA

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

Responsible University Administrator:
Matt Morton, Chief Information Security Officer

Responsible University Office:
Information Security

Policy Contact:
Information Security • security@unomaha.edu

Systems Access Control

POLICY CONTENTS

Scope

This policy applies to any university employee, contractor, or third party who has access to university information. This also applies to members of the faculty who are part of the Collective Bargaining Agreement between the NU Board of Regents and the University of Nebraska Omaha (UNO) Chapter of American Association of University Professors (AAUP).

This policy affects systems that are implemented on the UNO network or any system that in the course of standard business operations represents the university.

Policy Statement

Access Management

All computer equipment and media used for the generation, distribution, and storage of information used by the university are to be controlled and physically protected. The controls and physical protection in place must be commensurate with the classification designation of the information contained on the media or computer equipment. The controls and protection are in place to prevent damage to assets, minimize interruption to business activities, and protect confidential data.

Need to Know

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, policies, or attributes wherever possible and practical. The use of roles, policies, and attributes simplifies the administration of security by permitting access privileges to be assigned to groups of users versus individual users. Roles are established based upon department and job function and are reviewed and updated when job or departmental functions change.

Review of Administrative Rights
When a change to an individual's access privileges is needed, an Access Change form must be completed. Information from the forms will then be archived and maintained for a period of one (1) year and kept in secure storage. The privileges granted to all university employees will be periodically reviewed by information owners and/or custodians to ensure that university employees have access only to data that they have a need to know. Access control change forms and current system access control settings will be used during the review of access privileges for university employees.

Customary Separation
Email access is allowed through the communicated separation date, in consideration that the employee complies with all usage restrictions as communicated at the time of separation.

Exception guidelines are available in Appendix A: Employee Separation Procedures and Guidelines.

Identification and Authentication
University employees must provide valid identification before being granted access to university computing resources. For employees, this process is within the HR proofing process that completes the I-9 form. For members of the UNO AAUP Chapter, this process is performed by the hiring college Dean, Senior Vice Chancellor or their designate. For students, the proofing process is handled by the Office of the University Registrar.

Identification Assignment
Each user of university computing resources must be assigned a unique NetID for use during the authentication (login) process. Users are forbidden to share their NetID and will be held responsible for activities that take place using their user accounts. Users that have a need for privileged access are to use their standard account for normal access. When privileged access is required, system commands that allow change to active NetID or another user account will be used to gain the privileges that are needed to ensure the activity is logged. Refer to the UNO Identification and Authentication Policy (under development) for a detailed description of the handling of the NetID.

Shared access accounts are discouraged but in certain cases are necessary. Due to the risk inherent with shared accounts, additional controls need to be in place:

- Before a shared account is approved, alternatives that could help accomplish the objective without using a shared account are analyzed.
- Shared accounts are reviewed annually by the Information Security Office.

- Passwords for shared accounts must be changed when anyone with knowledge of the password leaves the organization or changes responsibilities and no longer requires access to the account.
- A systematic password change log must be established and managed.
- Access logs of the usage of the shared account must be created and reviewed on a periodic basis by appropriate personnel.
- Scripts containing passwords for shared accounts are only used when necessary, and must be secured from unauthorized viewing/modification. The scripts should contain an encrypted form of the password whenever possible.
- Upon a user's separation date, their access is revoked.

Dormant User Identification

User account usage must be automatically or manually reviewed to determine which users have not authenticated to information systems during the ninety (90)-day period prior to the review date. User accounts must be disabled if they have not been used for ninety (90) days.

Password Requirements

Where it is supported by operating system or access controls, users are given five (5) attempts for authenticating during a login session on the information systems before authentication is disabled or delayed. The following control settings for passwords must be used whenever possible and practical:

- Minimum password length of seven (7) characters
- Password expiration after ninety (90) days
- Passwords contain a combination of numeric and alphanumeric characters
- Password history maintained of at least four (4) different passwords
- Minimum password age of ten (10) days (to prevent rapid changing of password back to original)
- Unsuccessful password attempts limited to five (5)
- Account lockout of thirty (30) minutes
- Help Desk and Network Administrators can override the account lockout

The Information Services Help Desk personnel and/or administrators of university information system resources will assign user passwords during initial account setup and will reset passwords only when requested by account owners or the respective department security manager. Wherever systems software permits, passwords, assigned either as a new password for a new account or as a reset, must be valid only for the initial login. At that time, the system must force users to choose and set a different password for their account.

All passwords stored on university information systems or within applications and databases must be encrypted using a university-approved encryption algorithm. Under no circumstances may passwords be stored or transmitted in plaintext format. This includes batch files, automatic login scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Similarly, passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons may discover them.

Minimum Controls for Authentication Credentials

- Systems accessed using authentication credentials must not be left unattended in locations where unauthorized persons might gain access to them.
    - # 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

Workstations and terminals must be logged-off or locked prior to being left unattended for an extended period of time when applications with confidential information are active. Screensaver functionality must be enabled and configured to password-protect servers, workstations, and terminals after fifteen (15) minutes of keyboard/mouse inactivity for mainframe and LAN applications as well as web applications. Inactivity settings may be configured to shorter periods depending on user preference and information sensitivity. Settings must require password entry to unlock the screensaver. Passwords must meet university strength and composition requirements.

Network Access

Access to both internal and external networked services must be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring:

1. Appropriate interfaces between the university’s network and other external networks
2. Appropriate authentication mechanisms for users and equipment
3. Control of user access to information services

Network Trust

University employees must not establish connections with external networks (including Internet Service Providers) unless these connections have been approved by the Information Security Office. All inbound session connections to university computers from external networks (e.g. the Internet) must be protected with an approved password access control system. The university network perimeter must be defined. Information security requirements have been established for network connections to entities that exist outside the network perimeter.

Firewalls

Network devices performing firewall functionality must be configured to support a least-privilege approach to security, allowing only specific systems, services, and protocols to communicate through the network perimeter. All default operating system and firewall application security features must be reviewed and configured to meet this requirement. Logical and physical access to these systems

must be limited to those personnel with specific training and authorization to manage the device. Changes to firewall settings must follow change management policies and procedures.

Remote Access
Only virtual private network (VPN) technologies approved by the Information Security Office are permitted to be connected to the university network environment for remote access to systems that contain restricted data. All proposed changes or additions to any VPN configuration(s) must undergo a risk evaluation and have written approval from the CISO or their delegated representative.

Reason for Policy

Physical and logical access to information in the possession of, or under the control of UNO must be restricted to authorized individuals. This policy outlines the requirements for logical access controls with the intent of reducing the risk of unauthorized access to university information assets. This also outlines the procedures for removal of access with regard to employee separations. Detailed separation guidelines and checklists are identified in Appendix A: Employee Separation Procedures and Guidelines.

Procedures

Requesting Access to Electronically Store Regulated Data

To be granted access to electronically store regulated data, you must first complete the Regulated Data Authorization Form located in Appendix B of the UNO Regulated Data Security Policy.

Once the request form is completed and signed by an Academic Dean or Divisional Leader, then the request will be considered for authorization by the Regulated Data Authorization Committee. If a regulated data storage request is denied by the Regulated Data Authorization Committee, the requester may appeal to the Executive Regulated Data Authorization Committee. The Executive Regulated Data Authorization Committee will make the final decision. Reauthorization to continue to electronically store regulated data is required on a biennial basis.

Information Services (IS) provides a Regulated Data Server for any authorized individual or department to use. If the IS Regulated Data Server will not be used, the proposed storage location must meet the technical security requirements outlined in Appendix B of the UNO Regulated Data Security Policy.

Regulated Data Storage Requirements

Technical Requirements
All regulated data must be stored on the Regulated Data Server managed by IS unless an exception is granted as outlined within the UNO Regulated Data Security Policy. Updates will continue to be made to these requirements as technology and cybersecurity threats change. Authorized users will be notified as changes are made.

Audits
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 with this policy may result in disciplinary actions.

Definitions

Minimum Necessary/Least Privilege: The concept that all users at all times are to perform their job duties with as few privileges as possible.

Separation Date: Date at which employee separation becomes official.

Collaboration Tools: The tools provided for communication and collaboration. These include, but are not limited to email, instant messaging, phone, and voicemail.

Account: Typical access ID used for the access of applications and systems. For UNO this is usually the NetID.

Privilege: Access to university resources.

Base Administrative Access: Access to systems such as Firefly or MavLINK that provide access to tax documents, payroll information, transcripts, or any other entitlement not related to the management of systems.

Authentication Credentials: Identifying information that when used in conjunction with a password or passcode allows access to a protected resource.

Virtual Private Network (VPN): Protects data transfers between two or more networked devices so as to keep the transferred data private from other devices on one or more intervening local or wide area networks.

Shared Access Accounts (e.g. generic or general accounts): Allows multiple users to logon to the information technology resources using the same ID and password.

ISO 27002: Set of information security standards/practices that are used worldwide and managed by the International Standards Organization (ISO). This is the standard against which UNO measures itself.

University Administrative Designee: Senior Vice Chancellor, Vice Chancellor, or the Assistant to the Senior Vice Chancellor for Human Resources and Academic Affairs.

Related Information

Additional Contacts

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

Administrative Designee: Responsible for enforcement of this policy relative to faculty governance.

Chief Information Officer (CIO): Responsible for enforcing technology requirements outlined in this policy.

Chief Information Security Officer (CISO): Responsible for the enforcement of this policy as well as consulted on the determination of risk in conjunction with the Director of HR on matters of employee separation.

NU Executive Memorandum 16

NU Executive Memorandum 26

State of Nebraska Consumer Notification of Data Security Breach Act of 2006

UNO Security Manual

UNO Regulated Data Security Policy

Regulated Data Authorization Form

Employee Separation Procedures and Guidelines

Collective Bargaining Agreement – UNO AAUP Chapter

References

This policy addresses the following sections of ISO 27002:

11.1.1 Access control policy
11.2.1 User registration
11.2.2 Privilege management
11.2.3 User password management
11.2.4 Review of user access rights
11.3.1 Password use
11.3.2 Unattended user equipment
11.4.1 Policy on use of network services
11.4.2 User authentication for external connections
11.4.4 Remote diagnostic and configuration ports
11.4.6 Network connection control
11.4.7 Network routing control
11.5.1 Secure log-on procedures
11.5.2 User identification and authentication
11.5.3 Password management system
11.5.4 Use of system utilities
11.5.5 Session time-out
11.5.6 Limitation of connection time
11.6.1 Information access restriction
11.7.1 Mobile computing and communications
11.7.2 Teleworking

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.
