Policy Title

Systems Access Policy

Policy Information
- Date issued: 3/2/14
- Approved by: Chancellors Cabinet
- Last revision: 3/21/14

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. It also outlines the procedures for removal of access with regard to employee separations. **Detailed separation guidelines and checklists are identified in Attachment A.**

Responsibilities
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.

Entities Affected By This Policy

This document is intended for use as a guideline for any University employee, contractor, or third party who has access to University information from the adoption date going forward.

Members of the faculty who are part of the Collective Bargaining Agreement between the NU Board of Regents and the UNO Chapter of AAUP.

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

Retiring employees are not affected by this policy and maintain access to email and base administrative access within policy guidelines indefinitely.

Who Should Read This Policy

University supervisors, technical support staff and information asset stewards.

Access Management

All computer equipment and media used for the generation, distribution, and storage of information used by the University needs 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.

Privilege Assignment

Formal standards and procedures cover all stages in the life-cycle 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. Controlling 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 year, but access privileges are removed as described in the section labeled “Separation” 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 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.

Customary Separation

E-mail access is allowed through the communicated separation date, in consideration that the employee complies with all use restrictions as communicated at the time of separation.

Exception guidelines are available in Appendix A.

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 is the hiring college Dean, Senior Vice Chancellor or their designate. For students the proofing process is handled by the Registrar.

Identification Assignment

Each user of University computing resources must be assigned a unique Net ID for use during the authentication (logon) process. Users are not to share their Net ID and will be held responsible for activities that take place using their user accounts. Users that have a need for privileged access should use their standard account for normal access. When privileged access is needed, system commands that allow change to active Net ID or another user account should be used to gain the privileges that are needed to ensure the activity is logged. Reference the UNO Identification and Authentication Policy (under development) for a detailed description of the handling of the Net ID.

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 the users’ separation date, access is revoked.
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 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 in recognizing and reporting security violations related to authentication credentials.

Systems and Application Access

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:

- Identifying and verifying the identity, and if necessary the IP or location of each authorized user;
- Recording successful and failed system accesses;
- Providing appropriate means for authentication; if a password management system is used, it must ensure quality passwords;
- Where appropriate, restricting the connection times of users.

Remote Access

Only virtual private network 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 virtual private network configuration(s) must undergo a risk evaluation and have written approval from the CISO or their delegated representative.

Website Address for This Policy

http://www.unomaha.edu/policies

Related Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.nebraska.edu/about/exec_memo16.pdf">http://www.nebraska.edu/about/exec_memo16.pdf</a></td>
<td>NU Executive Memorandum 16</td>
</tr>
<tr>
<td><a href="http://www.nebraska.edu/about/exec_memo26.pdf">http://www.nebraska.edu/about/exec_memo26.pdf</a></td>
<td>NU Executive Memorandum 26</td>
</tr>
<tr>
<td>Under development</td>
<td>UNO Identification and Authentication Policy</td>
</tr>
<tr>
<td></td>
<td>Collective Bargaining Agreement – UNO AAUP Chapter</td>
</tr>
</tbody>
</table>

References

This policy addresses the following sections of ISO 27002:

11 Access control

This policy addresses the following sections of the UNO Information Security Manual:

Chapter 11 Access Control
Definitions

Minimum necessary/Least Privilege - The concept that all users at all times should run with as few privileges as possible, and also launch applications 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 email, instant messaging, phone and voicemail.

Account – typical access id used for the access of applications and systems. For UNO this is usually the Net ID.

Privilege – access to 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 item that when use with a password or passcode allows access to a protected resource.

Security Controls – procedures put into place that are related to securing access, and integrity of the resources in question.

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

Shared access accounts (i.e., 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). The standard by which UNO measures itself against.

University Administrative Designee – Senior Vice Chancellor, Vice Chancellor or the Assistant to the Senior Vice Chancellor for Human Resources and Academic Affairs
Attachment A

Employee Separation Procedures and Guidelines
Referenced from: Systems Access Policy

Normal procedures are as follows:

- If the separation is immediate and involuntary, all system access and collaboration tools are terminated on the communicated separation date from the HR Director (Staff) or the University Administration Designee for UNO AAUP Chapter members (Faculty).
- If the separation is not immediate or is voluntary, e-mail access is allowed through the communicated separation date, in consideration that the employee complies with all use conditions as communicated at the time of separation.
- Continued collaboration tool use by separated employees requires approval of the HR Director or Senior Vice Chancellor for Academic Affairs and Chief Information Security Officer (CISO).
- Separated employees are entitled to base administrative access to systems that deal with benefits, payroll and tax information. Refer to the Definitions section for a definition of this access.
- Retiring employees maintain access to email and base administrative access within policy guidelines indefinitely.

Voluntary/Involuntary – not immediate

Employee has all access removed on the separation date. HR will communicate with the separating employee regarding the separation conditions. In the event that the separation conditions, as outlined in the separation letter, are not followed access may be terminated sooner. After discussing with the employee supervisor to assess any risk the Chief Information Security Officer (CISO) or the Director of Human Resources in consultation with the Vice Chancellor may choose at their discretion to remove access prior to any communicated date.

All access to files, servers, social media, and shared service accounts are removed on the separation day. This day is identified and reported to Information Services (IS) by Human Resources (HR) or the University Administrative Designee. Access to the management of administrative data is also removed. Base administrative access is provided for access to all benefits, documents, etc. that are required dependent upon association with the University after separation. A list of services and their associated access restrictions is available within the UNO Identification and Authentication Policy (currently under development).

Involuntary - immediate

- Employee has collaboration tools and system access removed as soon as separation date is received by Information Security Office from HR.
- The ISO acknowledges the receipt of request and notifies HR or Administrative designee when complete. HR or the University Administrative designee acknowledges receipt of notification of completion.
- The employee’s manager, the University Administrative designee or HR Director may make a written request to ISO for a copy of all files to fulfill business continuity or legal requirements.
- The employee’s manager or the University Administrative designee may also request access to email for business continuity purposes. This may include a forward on the account or direct access depending upon the conditions of separation.
- A courtesy message will be placed on email notifying those outside the university that the individual is out and to contact their supervisor or the Administrative designee for specific questions.
- If personal files were kept in a folder marked “personal” then employees may be able to retrieve personal files with assistance from their manager. HR or the University Administrative designee will arrange the time and facilitate the transfer with assistance from information services.
- Depending upon the conditions of separation, where a staff member is expected to continue some duties prior to the communicated separation date, communication may be monitored and there is no right to privacy.
- All access to files and servers etc. are removed on the separation date. This day is identified and reported to the ISO by HR or the Administrative designee. In the event that the separation guidelines
are not followed by the separated employee, as specified from HR or the University Administrative
designee at the time of separation, access may be terminated sooner. The HR Director and CISO will
consult with the Vice Chancellor to assess any risk to the University and may choose, at their discretion,
to remove access prior to any communicated date depending upon the perceived risk.
- Access to the management of administrative data is also removed. Base administrative access is
provided for access to all benefits, documents, etc. that are required dependent upon association with
the University after separation. SAP is locked upon SAP security coordinator notice.
- Employee has 90 days of limited ESS access.

Employee / Student
In the event that the employee is a currently matriculated student the following steps will be executed.
- The email access will change over after the separation date from the current staff email system
(currently MS Office 365) to the student email system (currently Google Gmail (GMav)).
- No email messages will be migrated.
- Blackboard access will remain and be removed based upon current student access removal schedules
depending upon matriculation. The employee will be removed from any employee organizations or
groups within Blackboard.
- Firefly/ESS access will remain but only with the defined roles the affected individual is maintaining after
separation. For an employee who is a student this would mean that they would retain their student role
access to the system. Personal employee functions performed in ESS will be available 90 days after
separation.
- Limited Firefly/ESS access will be provided for 90 days.

External IT Services
All external IT service (social media, external web sites, etc.) account passwords will be changed and the
separating employee account will be removed unless continued use is authorized by the supervisor within the
conditions of separation.

Physical Access
Although the individual may retain the UNO ID card all access that is granted through the University proximity
card system is removed at the separation date.

University Property
All University property should be collected and noted within SAP under “Objects on Loan”. This includes any
property identified in Section 3.1.1.1 of the Collective Bargaining Agreement – UNO AAUP Chapter.

Special Exceptions
Employees may have multiple associations within the University including but not limited to student, alumni,
employment in a different division, etc. It is up to the manager to identify all additional employment or
associations within the University that may affect an involuntary separation. Prior to making the decision to
terminate, HR will advise the manager of all other appointments within the University system. In that context, a
determination of remaining access will be made by the manager in consultation with HR. IS will be notified of
the selected resources for which access will be removed. A list of services and their associated access
restrictions is available within the UNO Identification and Authentication Policy.

Before Separation:
- Please review the current inventory of systems and data access for the individual that you propose to
take some type of personnel action, which will end their employment at UNO. Information Services can
assist in gathering technology assets inventory when needed.
- Please review the “Separation Checklist” and indicate the access you want the person to have prior to
the decision to separate.
- Please identify specific dates that you want their access removed.

Questions that may impact the decision:
• Is the person being terminated for cause?
• Have you determined that you no longer trust this person to act in the University’s best interest?
• Do you fear that the person may destroy data, write inappropriate emails, disrupt business or challenge the reputation of the University?
• Do you want the person to be banned or barred from the facility or require notice before returning to campus?
• Is this a termination at will?
• Will the person continue to have responsibilities for completing assignments during the notice period?
• If so, what data or systems will the person need to complete the expected during the notice period?
• Do you want to have a snap shot of the files the day the notice will be given?
• Do you want them to be allowed to remove personal files from the system?
• Are some of the person’s duties being assigned to others during the notice period?
• If so, what access to systems will those assigned individuals need?
• Do you have concerns about any of the current data authority that this individual has?
• If so, what do you want to discontinue access to and when?
• Have you developed a letter of expectations for the notice period identifying specific duties and specific actions, which may negate the notice period and instead terminate for cause? i.e. if one has been developed, please provide copy to it.
• Please identify what monitoring you want done by IS, if any, to ensure they are complying with their separation conditions.

Separation Checklist

University Property:

Computer_______ Cell phone _______ Pager _______ Tablet ____________
Software_______ Tools _______ Manuals ______________
Uniform ______ Library books/materials _____________
Research equipment, data/databases: ________________
Purchasing Card _______________
Other: _______________

Access Codes & Keys:

Security/alarm codes/keys _____
Office keys ______
Desk Keys ______
Filing cabinet/furniture keys ______
Building access codes/keys ______
Departmental parking placard/key(s) _____________

Computer & Phone Access:

Unsubscribe from email distribution and list serves by notifying list serve owners ______
Notify IS of separation for account access removal ______
Notify SAP Team Lead for account access restriction ______
If moderator for list serves then reassign that control ______
Modify workflow routing ______
Change shared pass codes _____
Remove files from hard drive & server ______
Remove secondary security access ______
Update PeopleSoft (MavLink) system access ______
Update ESS/Firefly system access ______
Clear voice mail password ____ Purge messages _____
Review contents on network directories ______
Revise and remove as delegate on electronic calendar ______

Miscellaneous Office Issues to Address:
Reassign duties and/or projects in process ______
Determine location/access to all work related files ______
Reassign access to account(s) ______
Cancel Signature authority ______
Complete Change of Address form ______
Remove mail box/slot ______
Update departmental phone lists ______
Update employee databases ______
Update building or floor directories ______
All personal items are removed from work area ______
Submit employee’s final time record to Payroll ______
Confirm accurate transfer of any research accounts to another unit or institution: ______
Reconcile account & collect procurement card ______

**Employee Proximity Card Access is removed ______**