Access Control Policy (ISP-03)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all staff and contractors in IT, HR and Admissions who manage the onboarding of faculty, staff, contractors, and students.

Table of Contents

Introduction

To be able to control access to IT systems and the data that they store and process, it is critical that users are validated, access is authorized, and all connections authenticated to ensure the person or entity is who they say they are. This is a core principle and part of the Zero Trust philosophy. This ensures only approved entities have access to university data and systems.

Objective

This policy defines the requirements for user validation, entitlement definition, access authorization, and authentication throughout the user life cycle; from onboarding, through role changes to departure or termination. Thereby ensuring only authorized individuals and services can access company systems and information.

Policy Statement

General

Delivery of an effective and cost-effective end to end access control process requires the following to be in place:

1. All systems must utilize the University Single Sign-On (SSO) service (Azure AD) for user authorization and authentication. Exceptions to this are to be requested using the exception request process and routed to the CIO, CISO, or Qualified Individual (QI) for consideration.
2. All users are to be subject to an Identity Verification to confirm their identity.
3. All Staff and Contractors are to be subject to a background check as part of the hiring and onboarding process.
4. All requests for changes to or termination of access are to be authorized, and a record maintained. For Staff and Contractors this is done in SoftDocs and students via University ERP solution as part of the admissions process.
5. Every access request is to utilize a strong authentication mechanism.
6. Role-based access control is used to reduce administrative overhead and simplify audit activity.
7. The role of membership must be explicitly authorized. Implicit addition to roles based on organizational membership is not to be implemented for staff, faculty, and contractors. The fact that the user is part of a team is not sufficient justification to be added to that team's role.
8. System and data access is to be implemented to provide the minimum access required to perform a legitimate business function. Thereby following the security principle of "least privilege."
9. Under no circumstances are user IDs and passwords to be shared with anyone including colleagues or IT department members.
10. Student accounts will be maintained active for at least 1 year after the date of last attendance.
11. Service Accounts or non-human accounts are permissible and will not normally utilize the SSO system, but their credentials or secrets are to be stored in a secrets vault.
12. A registry of approved Service Accounts shall be maintained, including approver, responsible person, and the vault used to store the account secrets.

Onboarding

Onboarding is the process of providing an individual with access to the tools and knowledge necessary for them to perform their daily function, the steps that must be included during onboarding are as follows:

13. Validate the identity of the user as stated.
1. For Staff and Contractors perform a background check as defined by HR policy.
2. Line Managers or the Admissions department for students will authorize system access and define role or group membership.
3. All users will be required within 10 days of onboarding to review all applicable IT Security Policies.

Offboarding

Offboarding individuals promptly is critical to prevent inadvertent or malicious use of credentials and system access. Unused credentials are frequently used by rogue actors to gain a foothold or move laterally in an environment.

1. All offboarding and termination requests are to be documented within the SoftDocs or ticketing systems and implemented within 4 hours of the requested date and time.
2. Employment Services and management may from time to time require offboarding actions to be implemented immediately on the departure of a high-risk individual in these cases documentation after the fact is acceptable.
3. All offboarding actions are to be logged and monitored.

Technical Implementation

1. All computer resources capable of displaying a custom sign-on or similar message must display the following message as part of the login process:

This system is for the use of authorized users only. Users are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials

2. Local accounts are only permissible in exceptional circumstances and are to be registered as an exception to this policy.
3. This same validation authorization process is to be utilized for access to sensitive equipment rooms including those housing network equipment.

User Accounts

User accounts must adhere to the following guidelines:

4. Every user is to be allocated a unique user ID (UID) normally in the form of *InitialLastname.*
5. User IDs are never shared with users other than the owner.
6. Guest accounts are not permitted without written approval from the CISO.
7. Contracting and temporary employee accounts should expire on the final contract date
8. Password complexity and rotation rules as stated in the relevant policy are required.

Audit Trails

9. For compliance and compensating controls, all user provisioning, changes, and de-provisioning are to be logged along with the retention of all requests and approvals.
10. This material is to be retained for three (3) years at a minimum.
11. Logs are to be stored on a system that supports the requirements for legal chain of custody which includes non-repudiation should such information be required in court of law.
12. Audit artifacts are to be maintained documenting the approval/authorization process.

13. Log information should also include privilege authorizations, and role modifications for access to information systems.

Periodic Audits

Periodic audits of privilege user access are to be completed at least every 6 months to ensure only those individuals with a legitimate business need have access to sensitive PII, financial and business data and systems and that the principle of least privilege is being adhered to. These audits are a critical compensating control to counteract the fact that implementation of this policy is dependent on manual actions by several teams. This will require a review of all privilege users to ensure the following:

14. They are still legitimately employed or engaged by the university.
15. That all additions and changes to user access are authorized by the line manager/supervisor and the role manager, and that proper audit information exists to that effect.
16. That all changes and access removal requests were completed within one business day of the request.
17. Only those individuals with valid business requirements are assigned to each role.
18. That the list of directly administered systems that do not make use of the SSO solution is correct, and that justifications for the same are current.
19. Review the use requirement for password or secrets rotation of all system accounts.

Roles and Responsibilities

Delivery of a coherent end-to-end user access control system relies on many individuals across the university. Each group has specific responsibilities as outlined below:

Employment Services and Student Admissions:

20. Performing background checks as necessary on Staff and Contractors.
21. Validating the individual as the legal person through a passport, driving license check, or similar during the onboarding process.
22. Submitting the ID creation request along with device fulfilment request as needed to the End User Computer or standalone management team.
23. Submitting changes to role allocations on any changes in employment or work type.
24. Submitting offboarding and user removal requests is ideally ahead of a termination date. That request must include a due date for termination to occur. Maintaining auditable records of above and role approvals by Line Manager

End User Support Team – where a system is not utilizing the SSO solution, this also applies to that system's administration team:

1. Creating automation to perform the following:
    a. Create and deliver audit reports showing user allocation to Roles
    b. Create and deliver audit reports showing any accounts not deleted withing 4 hours of requested date and time.
2. Suspending any account that has not been used in the last 45 days
    a. Create and deliver audit reports of suspended accounts
3. Configure access rights and policies to match those specified by the role manger
4. Implementing password, logging, hardening and other policies as defined in the IT security Policy repository.
5. Authenticating users prior to initiating any change request particularly password change