Policy	Access Control Procedures
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	February 7, 2024
Reviewed	June 23, 2025
Approved by	VP for Finance and Administration
Version	25.1

ACCESS CONTROL PROCEDURES

PURPOSE

Shepherd University's Access Control Procedures are intended to assist departments and employees in understanding how to request new employee access and modify current employee access. This access includes, but may not be limited to, Active Directory, Wi-Fi, Email, Banner, and Argos.

Shepherd University adheres to the policy of "least user privilege" in assigning and maintaining account access for all employees, meaning that users are granted only the account permissions and access necessary to perform their current role. As a security methodology, "least user privilege" assists in preventing and/or limiting the scope of any data or account compromise.

PROCEDURES

NEW ACCOUNT PROVISIONING

When an employee is hired, HR will notify IT Services of the employee's name, department, and hire date. IT Services will use this information to create the user's Active Directory account and Email by their first day of employment.

ACCESS PROVISIONING

When a user requires new or updated access to any IT system, the request must be made by the user's supervisor. The request must include, at minimum:

- The name of the user requiring access or modifications
- The specific access needed or modifications to be made
- Any time limits to access

A user should not request or grant their own access. In the cases of functional overlap, the immediate

supervisor should be consulted, and the situation documented.

Termination of access rights should be done as soon as possible when notification is sent to IT Services, for either terminated or transferred employees.

- HR is responsible for notifications regarding terminated users, and IT will process these within one business day of receipt.
- Data custodians are responsible for notifying IT Services of access changes resulting from job changes, transfers, promotions, etc. IT will process these changes within one business day of receipt.

USER ACCESS REVIEW

User access review will be conducted once per year by the Data Custodians, facilitated by IT Services. IT Services will generate a report of current access by user and distribute to the Data Custodians, who will review and return any changes for processing.

User accounts should not be shared for systems that store sensitive data. In the case where "group" user accounts are necessary, they should not be granted access to such systems. Refer to the Acceptable Use Policy and Data Classification Policy for further details.

Individual user accounts should not be granted administrator-level privileges. Only accounts designated as Administrator-level accounts should be granted said permissions.

PASSWORD REQUIREMENTS

Passwords to all campus systems that store sensitive or protected data should adhere to accepted best practices for password complexity and length.

SCOPE of AFFECTED PARTIES

This policy applies to all employees, whether full- or part-time, including Emeritus employees who are granted limited account access (e.g. email), and said employee supervisors and department heads.

ROLES & RESPONSIBILITIES

All Shepherd University students, faculty, staff, and other parties with access to Shepherd University information assets and IT resources shall be responsible for:

USERS

- Understand and comply with the guidance provided by this policy, as well as applicable compliance programs and associated awareness training, including laws, standards, procedures, and university protocols.

- Supervisors of new and transferred employees should ensure adequate training is provided to protect their user accounts and safeguard sensitive or protected data to which they may access (e.g. FERPA training).
- HR and Data Custodians are responsible for timely notification to IT Services regarding hiring, termination, or changes in employee roles requiring access changes.
- Promptly report any suspected violation of this policy, any security events, and/or incidents involving a suspected compromise of a user's account or IT resource to itworkorder@shepherd.edu.

CIO/CISO - INFORMATION PRIVACY OFFICER

- Oversee and administer this policy.
- Provide authorization and direction to IT Services staff in accordance with this policy.
- Develop awareness and necessary training materials as it pertains to this policy.

IT SERVICES STAFF

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.
- Ensure all associated procedures are followed and documented accordingly when taking any actions outlined in this policy.

RELATED TOOLS

TRAINING

- Family Educational Rights & Privacy Act (FERPA) Training
- Gramm-Leach-Bliley Act (GLBA) Training

RELATED POLICIES & GUIDELINES

- BOG#35: Information Technology Security
- Acceptable Use Policy
- IT Information Security & Privacy Policy
- Information Security Program