Policy	Information Security Program
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	February 7, 2024
Reviewed	June 26, 2025; May 14, 2026; June 24, 2026
Approved by	Provost and Vice President of Academic Affairs
Version	26.1

INFORMATION SECURITY PROGRAM

PURPOSE

Shepherd University's Information Security program is comprised of policies, network and security architecture, and current IT procedures and practices. It is an iterative process that, holistically, reflects an Information Security Program that is designed to provide technical and operational safeguards and mitigate risks regarding the storage and processing of sensitive and protected data, as described in the Data Classification Policy. Furthermore, it is designed to ensure the confidentiality, integrity, and availability of student and employee systems and data.

Shepherd University adheres to the philosophy of "Defense in Depth," a practice which implements several layers of protection to contribute to an overall security posture. These include

1. Physical access controls
2. Logical access controls
3. Perimeter, network, and server security
4. Penetration testing and tabletops in cooperation with external partners
5. Third party data security agreements for external vendors
6. Employee training and awareness

By implementing an effective Information Security Program, the University demonstrates its commitment to safeguarding sensitive and protected data and mitigating the risk of security incidents.

PROGRAM DESCRIPTION

A periodic CIS CSTAT risk assessment forms the basis for the development, evaluation, and modification of the Information Security Program. The results of these risk assessments are reviewed with Executive Leadership.

The Information Security Program informs and influences the following.

- Design and implementation of safeguards to mitigate and address identified risks to sensitive and protected data. See Data Classification Policy.
- Policies and procedures, such as Access Control Procedures.
- GLBA compliance activities and procedures
- Oversight of information system service providers.
- Consultation on projects that relate to data security.

In addition to the yearly CIS CSTAT risk assessment, risks may also be identified through the use of external audits, penetration testing, review of logs and similar activities. Shepherd University works with external cybersecurity providers to conduct two tabletop information security reviews per year, and a penetration test every 3year. The outputs of these activities inform the creation and modification of the Information Security Program. The University reviews its Information Security Program yearly in order to ensure that changes and newly identified risks are accounted for.

The Office of the CIO/CISO also acts as a resource for campus project management to ensure that security is accounted for throughout the project lifecycle. The Office of the CIO/CISO also conducts a review of vendor contracts and new installations to ensure that they meet security requirements.

GLBA Compliance Procedures

Policy

Section 314.4 of the Safeguards rule identifies the following elements to be addressed. Shepherd University's approach to each element is described below.

Designate a qualified individual to implement and supervise your company's information security program

The director of IT Services also serves as the CTO/CISO and qualified individual.

Conduct a risk assessment

See Risk Management Policy

Design and implement safeguards to control the risks identified through your risk assessment

1. Implement and periodically review access controls
   See Access Control Procedures
2. Know what you have and where you have it
   See Data Inventory Policy

3. Encrypt customer information on your system and when it's in transit
   See Data Encryption Policy
4. Assess your apps
   Shepherd University does not develop apps in-house
5. Implement multi-factor authentication for anyone accessing customer information on your system
   MFA is currently implemented for Office365 and Ellucian Banner Application Navigator
6. Dispose of customer information securely
   See Data Disposal Policy
7. Anticipate and evaluate changes to your information system or network
   See Change Management Policy and Risk Management Policy
8. Maintain a log of authorized users' activity and keep an eye out for unauthorized access
   We have logs created by Active Directory and operating systems. However, due to resource limitations, we do not have a log aggregation tool or similar.

a. Regularly monitor and test the effectiveness of your safeguards
   The last penetration test was completed January 2026
b. Train your staff
   We use Proofpoint for phishing simulations and employee cybersecurity and GLBA training
c. Monitor your service providers
   See Vendor Management Policy
d. Keep your information security program current
   This document is reviewed and updated yearly
e. Create a written incident response plan
   Incident Response plan available on request
f. Require your qualified individual to report to your Board of Directors (at least annually)
   Reporting occurs annually

POLICIES AND PROCEDURES

Current versions of policies, procedures, and guidelines can be found on the IT Services Policies and Procedures page, https://www.shepherd.edu/itservices/itspandp

SCOPE of AFFECTED PARTIES

This policy applies to all users, such as students, faculty, and staff of Shepherd University and to other persons accessing Shepherd University information assets and/or IT resources including but not limited to authorized agents or community members, regardless of whether such information asset or IT resource is accessed from on-campus or off-campus.

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 affiliated awareness training with all applicable laws, standards, procedures, and university protocols.
- Physically secure and safeguard information assets and IT resources, within the user's possession and control, including abiding with the safe handling of data.
- 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.
-

RELATED TOOLS

TRAINING

- Gramm-Leach-Bliley Act (GLBA) Training

RELATED POLICIES & GUIDELINES

- BOG#35: Information Technology Security
- Acceptable Use Policy
- IT Information Security & Privacy Policy
- Access Control Procedures
- Password Policy