Policy	Information Security & Privacy Policy
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	August 18, 2021
Reviewed	April 25, 2025; May 14, 2026; June 24, 2026
Approved by	Provost and Vice President of Academic Affairs
Version	26.1

INFORMATION SECURITY & PRIVACY POLICY

PURPOSE

Information assets including data, computing devices, systems technology, telephony, and IT resources are vital to Shepherd University's ongoing mission of discovery, learning, and engagement. All information assets and IT resources must be protected throughout various phases of their useful life, including when created, collected, stored, transferred, purged, and ultimately destroyed. To support its mission, Shepherd University requires certain administrative, technological, and physical safeguards must be in place to adequately protect information assets and IT resources.

POLICY

Shepherd University information assets including data, computing devices, systems technology, telephony, and IT resources shall be used in an approved, ethical, and lawful manner to avoid loss and/or damage to Shepherd University data, operations, image, or financial interests. All affiliated information/technological data should be considered as confidential and proprietary, thus every effort to protect its integrity should be made.

A trusted, secure, and effective IT environment is vital to the continuing success of Shepherd University; thus, we will:

1. Establish, sustain, and control a secure IT environment consisting of internal controls designed to maintain, facilitate, and promote adequate protection of information assets and IT resources through standards, protocols, policies and guidelines, and training.
2. Identify and classify information assets and IT resources according to their use, sensitivity, and importance to Shepherd University and in compliance with federal and/or state laws.
3. Facilitate collaboration and communication among stakeholders, data custodians, and members of the campus community to aid in protecting information assets and IT resources, with the recognition of the ability to quickly adapt to emerging technologies.

4. Ensure that access to information assets and IT resources is governed by effective role-based access controls, managed by the Director of IT Services / Information Privacy Officer, that enables users to fulfill the responsibilities of their position.
5. Manage risks to information assets and IT resources through appropriate administrative, technological, and physical controls to protect from unauthorized access or modification, misuse, or damage.

Use of information assets and IT resources is a privilege and not a right. All users are responsible for the actions performed on or transmitted with any Shepherd University information asset and/or IT resource. Violations of this policy, or any other Shepherd University policy, may result in revoked or limited technology privileges, as well as other disciplinary action up to an including expulsion, termination, or referral to appropriate authorities.

PRIVACY, OPERATIONS, and MONITORING

Shepherd University seeks to maintain its IT environment and manage all information assets including data, computing devices, systems technology, telephony, and IT resources in a manner that respects individual privacy and promotes user trust. However, the use of Shepherd University IT resources is not completely private, and users should have no expectation of privacy in connection with the use of any information asset or IT resource.

Shepherd University has the legal right to access, preserve, and review all information stored on or transmitted through any information asset or IT resource, including the inspection of e-mail message, logging of activities, monitoring usage patterns, and data audits/integrity checks. IT Services may, with or without notice to users, take any other action it deems necessary to preserve, secure, and protect systems, information assets, or IT resources for the betterment of Shepherd University. Without limiting its right to take action, Shepherd University may, at its sole discretion, disclose the results of any general or individual monitoring or access permitted by this policy, including the contents and records of individual communications, to appropriate Shepherd University personnel and/or law enforcement agencies.

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:

<u>USERS</u>

- Usage of all information assets and IT resources in compliance with all applicable laws and Shepherd University policies, standards, guidelines, regulations, and procedures.
- Physically secure and safeguard information assets and IT resources within the user's possession and control, including abiding with the safe handling of data.
- Understand and comply with the guidance provided by this policy, as well as applicable compliance programs and affiliated awareness trainings.

- 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.
- Ensure all requests to access or disclose information per policy is reasonably required in order to protect Shepherd University interest, is properly authorized, and meets the scope and conditions of permitted access.
- Provide authorization and direction to IT Services staff in accordance with this policy, to authorize disconnection of any information asset and/or IT resource or disabling of a user account if it is believed that either is compromising the information security and privacy of Shepherd University.
- Authorize the discontinuation of application development or deployment efforts if it is found during a risk assessment that the impact of a particular risk, threat, or other privacy matter is likely to compromise the information security of Shepherd University, until a remedy is implemented to mitigate said issue.
- 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
- E-mail Policy
- Data Classification Policy
- Data Notification Policy
- International Travel Security Policy
- Password Guidelines
- Social Security Number Guidelines
- Work from Home / Remote Access Guidelines
- Access Control Procedures
- Information Security Program