Policy	SSN Guidelines
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	August 18, 2021
Reviewed	June 23, 2025
Approved by	VP for Finance and Administration
Version	25.1

SSN GUIDELINES

PURPOSE

Shepherd University is dedicated to ensuring the privacy and proper handling of social security numbers (SSNs) of its students, faculty, staff, and affiliates.

GUIDELINES

Shepherd University remains steadfast in ensuring those users who handle or have access to SSN are properly aware of the increased confidential emphasis on secure use, transmission, and storage of SSNs throughout Shepherd University IT resources.

It is Shepherd University's intent to protect the SSN of its students, faculty, staff, and affiliates to minimize the growing risks associated with identity theft by collecting the SSN only as:

1. Required by law.
2. When necessary for employment records, admission records, financial aid records, and a limited number of other business and governmental transactions, as required by law.
3. As a means to uniquely identify an individual for a Shepherd University ID number (SUID) assignment.
4. A method to identify individuals for whom a SUID has been created and not used for other internal processes.

Shepherd University will assign a SUID to an individual upon initial association with the university. The SUID is not the same as, nor based upon, the individual's SSN or any other unique demographic information. The SUID will be used in all future electronic and paper data systems to identify, track, and service individuals associated with Shepherd University. The SUID will be permanently and uniquely associated with the individual to whom it is originally assigned. The SUID will be considered the property of Shepherd University and its use and governance will be at the discretion of Shepherd University, within the parameters of the law.

SSN is not be used as a common identifier or used as a database key in any Shepherd University IT resource.

PRIVACY, OPERATIONS, and MONITORING

Shepherd University is dedicated to ensuring the privacy and proper handling of social security numbers (SSNs) of its students, faculty, staff, and affiliates.

- All Shepherd University forms and documents that collect SSNs will use the appropriate language to indicate whether request if voluntary or mandatory.
- Those departments that handle or have access to SSNs will be adequately trained regarding appropriate use, disclosure, and data handling of SSNS prior to accessing Shepherd University information assets or IT resources.
- SSNS will be transmitted electronically only through strong, data-encrypted mechanisms.
- Paper and electronic documents containing SSNs will be disposed of in accordance with data handling requirements as defined by the administrative data owner and/or the Information Privacy Officer.
- All new technological or logical systems purchased or developed will not use SSN as an identifier, except where such use is specifically permitted or required under this guideline. Such systems will not visually display the SSN on any system output, including monitor/display or printed forms, unless required by law or by Shepherd University in execution of its duties.
- No public display of personal information will be posted in a manner where a whole or partial SUID or SSN are used to identify an individual.

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 messages, 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 specifically to those users who have access to collect and/or handle SSNs. However, all users need to have a general awareness of this affiliated guideline.

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:

AUTHORIZED USERS / DATA STEWARDS / BANNER CUSTODIANS

- Understand and comply with the guidance provided here, as well as applicable compliance programs and affiliated awareness trainings.

- Comply with these guidelines in daily operations/interactions with the campus community.
- Promptly report any suspected violation or breach of confidentiality, along with any security events, and/or incident to itworkorder@shepherd.edu

CIO/CISO - INFORMATION PRIVACY OFFICER

- Oversee and administer this guideline.
- Provide authorization and direction to IT Services staff in accordance with development of system-generated SUID.
- Facilitate the review of requests for a security policy exception.
- 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
- Information Security & Privacy Policy
- Technological Remote Access Guidelines