| | |
|---|---|
| Policy | Data Encryption Policy |
| Impact | Data, Technology, and IT Resources |
| Responsible Office | IT Services |
| Created | June 4, 2025 |
| Reviewed | June 23, 2025 |
| Approved by | VP for Finance and Administration |
| Version | 25.1 |

# DATA ENCRYPTION POLICY

## PURPOSE

Shepherd University's Data Encryption Policy is intended to establish standards for data encryption at rest and in transit. Please see Data Classification Policy for further information and definitions.

## POLICY

### Banner System

Banner data is encrypted both at rest and in transit using AES-256 encryption. SSL certificates are employed for application servers.

### Email

Restricted, confidential, or sensitive data should not be sent in email or as an email attachment. This data may be stored on Shepherd University network drives or on Shepherd University Office 365 OneDrive and shared using those technologies when necessary as they meet University encryption standards.

### Portable Devices

It is strongly recommended that users avoid storing any restricted, confidential, or sensitive data on portable drives or devices.

## SCOPE OF AFFECTED PARTIES

This policy applies to all users such as students, faculty, and staff of Shepherd University accessing Shepherd University information assets.

## ROLES & RESPONSIBILITIES

CIO/CISO – Information Privacy Officer

- Oversee and administer this policy.
- Provide authorization and direction to IT Services staff in accordance with 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

Data Classification Policy