Policy	Risk Management 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

RISK MANAGEMENT POLICY

PURPOSE

Shepherd University's Risk Management Policy is intended to establish a framework for identifying, evaluating, monitoring, and responding to risks to university systems and data, as well as support strategic decision-making.

POLICY

Risk Identification

IT staff will conduct a yearly risk assessment using the CIS CSAT model. This assessment will provide the basis for the IT risk assessment. In some cases, additional risks may be identified through alternate means.

Risk Assessment

Led by the CIO, IT staff will assess the identified risks based on likelihood and potential impact.

Risk Prioritization and Mitigation

Risks will be prioritized and mitigation strategies will be identified based on the risk assessment and resources available. In some cases, risk may be accepted due to the results of the assessment, limited resources, or both.

Results of the risk assessment and prioritization will be shared with upper management. This information will be used to inform decision-making relating to IT priorities for the coming year/s.

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.
- Coordinate with IT staff to develop policies and procedures to address risks

IT Services Staff

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.
- Participate in yearly risk assessment

RELATED

IT Information Security & Privacy Policy