UNIVERSITY OF

Effective: *08/08/2022*
Last Revised: *08/08/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-13: Risk Management Standard

Policy Contents

Risk assessments should consider the probable frequency (or likelihood) and impact (or magnitude) of losses. Potential forms of loss to consider include but aren't limited to:

4.3.2 Vulnerability Remediation or Quarantine

Vulnerabilities identified from scanning, testing, and monitoring activities must be reviewed by University IT Security Services personnel. Vulnerabilities must be prioritized by risk, assigned ownership, and remediated in accordance with established remediation timelines based on vulnerability criticality:

Vulnerability Compliance Time line		
Severity	Remediation Time Frame	POAM / Quarantine Determination
Urgent (Zero-Day / As-Directed)	7 calendar days	CISO Directed
Critical	15 calendar days	

4.4 Third Party Risk Management

4.4.1 Vendor Due Diligence

A Vendor Risk Assessment will be conducted before The University undertakes any activities with a vendor that involves processing of high-risk data or access to IT systems. Vendor Risk Assessments must:

- Identify services/solutions to be provided by the vendor, based on the proposed scope of work, that require access to high-risk data and IT systems
- Document reasonably foreseeable internal and external risks to security, data and privacy posed by the vendor and its services/solutions
- Provide recommendations to remediate or mitigate risks
- Verify capabilities of the vendor to ensure their ability to deliver their services/solutions in compliance with University