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-14: Security Assessment Standard

Standard Contents

1. Purpose

The purpose of the Security Assessment Standard is to define the organization's requirements for enforcing effective Security Control Implementation and Assessment procedures to effectively mitigate against information security risks and validate ongoing mitigation effectiveness. This standard serves as a statement of objectives for implementing and performing security assessments against University owned assets.

2. Scope

This standard shall apply to all The University of Nebraska ("The University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this standard.

3. Standard Statement

It is the intention of this policy to establish a security control framework and form assessment procedures and guidelines for administering assessments amongst University assets. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer ("CISO") as defined in **ITS Policy Exception Standard**. The following subsections outline the Security Assessment Standard.

4. Security Assessment Requirements

4.1 System Security Planning

4.1.1 System Security Plan

The University must develop System Security Plans (SSP) for information systems that process High Risk data, based on defined risk categorization. System Security Plans must be created and validated by the CISO prior to system implementation to ensure alignment with minimum security requirements. Plans should be treated as living documents and must be periodically reviewed and updated following significant changes to the information system and at least annually.

4.1.2 System Security Plan Minimum Elements

At a minimum, System Security Plans must include:

- System boundaries, interfaces, and data flows
- Laws, regulations, and policies affecting the system as well as security standards and guidelines
- Security requirements based on performed risk assessment
- Detail on how security requirements are implemented, including compensating controls and special circumstances.
- Role and responsibilities of security personnel
- High-level diagrams that show how connected systems talk to each other
- Design philosophies (defense-in-depth strategies, allowed interfaces, and network protocols)
- Inventory records must be reviewed and updated by the system owner annually and after significant changes to ensure that the inventory remains complete and accurate.

4.2 Application Development

4.2.1 Secure Code Training

Developers responsible for creating custom-developed software must complete secure coding training on an annual basis to ensure ongoing knowledge of secure coding practices and code-based vulnerabilities.

4.2.2 Secure Code Guidelines
Custom-developed software must be developed in alignment with established secure coding guidelines. These guidelines must be developed to align with industry best practice secure coding frameworks (e.g. OWASP, SANS, etc.). Guidelines must be periodically reviewed and updated to ensure ongoing alignment with new and emerging threats.

4.2.3 Secure Coding Reviews
Secure code reviews will consist of both static and dynamic code analysis. These analyses should be performed using both automated and manual processes to identify vulnerabilities. Secure code reviews must be performed on all custom-developed code prior to deployment to identify code level vulnerabilities. Secure code reviews must be performed by independent personnel not involved in the development of the code base. High risk vulnerabilities must be remediated prior to deployment. All other vulnerabilities must be addressed in alignment with the **Risk Management Standard.**

4.3 Control Assessment

4.3.1 Control Framework
The University has adopted the NIST controls as its information security control framework to ensure control coverage over all applicable regulatory and contractual obligations related to information security. This control framework will be periodically reviewed and updated by management to ensure ongoing appropriateness of coverage based on performed organizational risk assessments and regulatory changes.

4.3.2 Control Testing / Evaluation
Where possible a continuous monitoring capability will be used to ensure a frequent security assessments and analysis of vulnerabilities and threats is conducted. Where continuous monitoring is not possible, security assessments must be completed at least annually through manual or automated methods, to validate the operating effectiveness of implemented technical and process-based security controls. For each control in the NIST framework, The University must define the frequency of testing, testing method, and maintain the assessment results.

4.3.3 Control Assessment Remediation
Deficiencies identified during security assessments must be tracked on the risk register and remediation plans documented in a Plan of Action and Milestones (POAM) document in accordance with the **Risk Management Standard**.

4.3.4 Penetration Tests
Penetration tests must be performed on University information systems at risk-based, organizationally defined frequencies to test the adequacy of implemented information system security controls. Identified vulnerabilities must be remediated in accordance with the **Risk Management Standard**.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	08/08/2022
Approved by:	Bret Blackman	IT CIO	08/08/2022

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published