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-16: System and Communication Protection Standard

Standard Contents

1. Purpose

The purpose of the System and Communications Protection Standard is to assist in managing risks regarding vulnerable system configurations, denial of service, and data communication and transfers. The standard establishes an effective System and Communications Protection program, of which assists in the implementation of security best practices regarding system configuration, data communication, and transfers.

2. Scope

This standard shall apply to 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

4.1.5 Remote Access

External access to internal information system resources must be facilitated through the use an approved Virtual Private Network (VPN) connection, in alignment with the **Access Control Standard.** Remote access to virtual desktop environments must be performe

4.4 System and Application Security

4.4.1 Secure System Development

Development of custom software must follow approved University software design life cycle (SDLC) methodologies. All custom-software development must be developed following industry secure coding best practices (e.g. OWASP) and must incorporate security throughout the SDLC.

4.4.2 Security Architecture

All systems should be securely architected in alignment with University enterprise architecture standards. During the design phase, all system plans should be reviewed against secure architecture standards to ensure that all security requirements are considered and integrated into the development of the system.

Where applicable, all systems must utilize an N-tiered architecture to segment and separate application functionality between the web tier (De-militarized zone), Application tier, and data tier.

4.4.3 Secure System Configuration

University infrastructure used in the delivery of IT systems and services within the University network must be securely engineered and configured in alignment with the **Configuration Management Standard**. All University endpoints and systems must adhere in prohibiting remote activation of collaborative computing devices, such as cameras and microphones.

4.4.4 User Functionality

Systems must separate user functionality, including user interface services, from IT administrative functionality and interfaces. All access to administrative functions must abide to identification and authentication principles established within the **Access Control Standard.**

4.4.5 Mobile Code

Acceptable and unacceptable mobile code and mobile code technologies (such as javascript, HTML5, VBScript, etc.)

4.5.2 Data at Rest Encryption
Data must be encrypted at rest using secure approved secure algorithms in alignment with the **NIST Cryptography Standard.** Additional defense in depth strategies must be implemented to prevent unauthorized access and exfiltration of data, including strict access control and security monitoring.

High Risk data must not be stored on unauthorized assets or network locations, including public cloud storage, unauthorized removable media, or posted to public-facing websites in alignment with requirement **4.3.2** of this standard.

4.5.3 Data in Transit Encryption
Data must be encrypted in transit when transmitted over all public and internal networks. When sent via email, users are responsible for employing appropriate encryption measures. Encryption methods must utilize approved secure algorithms in alignment with the **NIST Cryptography Standard.**

4.5.4 Key Management Procedures
Key management procedures must be established for each key to establish roles and responsibilities for the secure

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,