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 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 standard to establish System and Communications standards throughout The University to help document and communicate best security practices in system configurations, data transfers, and communication. 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 System and Communications Protection Standard.

4. System and Communication Protection Requirements

4.1 Network Security

4.1.1 Network Segmentation

Subnetworks for publicly accessible system components must be physically or logically separated from internal networks, via a DMZ or segregated environments. All incoming traffic, irrespective of source type or connectivity method, must flow through University-managed security infrastructure.

Additionally, all inbound internet-sourced traffic must terminate at a DMZ.

4.1.2 Network Traffic Restriction

Systems must control communications at the external boundary of the system, between any DMZ and the internal network, and at key internal boundaries within the network. All network traffic control mechanisms must be configured to default deny-all traffic. All active ports and protocols must have a valid business purpose and must be formally approved and documented prior to implementation.

All firewall and network traffic filtering rules must be reviewed on an annual basis to verify ongoing business need.

4.1.3 Network Traffic Monitoring

All inbound, outbound, and network segment-traversing network traffic must be configured to process through University-managed security monitoring solutions. This traffic must be monitored for anomalous activity in alignment with the **System and Informational Integrity Standard.**

4.1.4 Remote Administration Session Encryption

All remote administration of network devices must be performed by authorized system administrators via secure connection through an encrypted session (e.g. Secure Shell). All access should be securely authenticated and authorized in alignment with the **Access Control 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 performed using secure configurations of remote desktop protocol and secure shell (SSH) bastion hosts.

4.1.6 Network Disconnect
Network connection must be automatically terminated following the end of the session or after a defined period of inactivity, after which point the user must be required to re-authenticate.

4.1.7 Session Authenticity
Authenticity of communications sessions must be protected to combat against man-in-the-middle and session hijacking attacks. Systems must be engineered to use sufficiently random mechanisms and approved session management frameworks. All sessions over public and unsecured networks must utilize secure transmission protocols (e.g. secure versions of TLS, SSL, etc.).

4.1.8 Split Tunneling
User devices connecting to University networks and systems via remote access must be restricted from simultaneously connecting to other security domains such as the public network or the internet (i.e., split tunneling).

4.1.9 Voice over Internet Protocol
Usage restrictions and implementation guidance must be implemented for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information asset if used maliciously. Monitoring and overall management of VoIP technologies must be performed to mitigate potential incidents.

4.2 Network Management

4.2.1 Network Segment and Connection Inventory
An inventory and system diagram of all network components must be maintained by Network Engineering teams. External connections must be formally approved prior to connection, inventoried, and periodically reviewed to ensure ongoing business need.

4.2.2 Wireless & Wired Networking
All wireless networking devices that connect or provide access to University networks must be hardened in alignment with the **Configuration Management Standard** and utilize authenticated and encrypted sessions, in alignment with the **Access Control Standard**.

Wired connections must enforce secure authentication, in alignment with the **Physical Protection Standard**.

4.2.3 Network Capacity Planning
Network administrators must periodically monitor network utilization, forecast future need, and communicate forecasts to appropriate stakeholders to ensure ongoing network capacity and availability.

4.3 Web Security

4.3.1 Domain Name System (DNS)
A University-managed Domain Name System (DNS) infrastructure must be implemented to block specific websites or IP addresses from malicious activities.

4.3.2 High Risk Data Restrictions
Communication and standards must be in place to restrict the publication of High Risk Data on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter). This policy applies to business related and personal posts relating to University High Risk Data.

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.) must be documented for business systems, where applicable as a known technology. These mobile codes must be restricted by usage and must be monitored and controlled within the information asset.

4.4.6 Information in Shared Resources

Where University applications and information systems process sensitive information utilizing shared memory with other systems, segmentation must be implemented though file permission restrictions, logical segregation, or similar protection methods.

4.5 Cryptography and Key Management

4.5.1 Cryptography Usage

Cryptographic mechanisms must be implemented to protect integrity of information, to include cryptographic hash functions in digital signatures, checksums, and message authentication codes. Encryption must be implemented based on data classification, in accordance with the following schedule:

Data classification	Requirement for encryption at Rest	Requirement for encryption in transit
High Risk (Non-Public)	Encryption required	Encryption required on public and internal networks
Medium Risk (Non-Public)	Encryption required	Encryption required on public and internal networks
Low Risk (Public)	Encryption required	Encryption not required

Additional protection mechanisms may be necessary depending on compliance or regulatory requirements for business or research needs. Refer to **Executive Memorandum 41** and **Executive Memorandum 42** for additional information regarding data classifications and handling requirements.

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 generation, management, and retirement of keys. Procedures must be periodically reviewed and updated by the key owner. Key procedures, at a minimum, must address:

- Secure key generation and distribution
- Registration
- Use
- Access
- Backup
- Secure storage
- Recovery
- De-registration
- Destruction

4.5.5 Dual Knowledge and Split Control

Dual control requires two or more people to perform an action. Split knowledge is a method in which two or more individuals separately maintain control of key components and where each individual only knows their own key component.

Where possible, management of encryption key material should be controlled based on split knowledge and dual control. Dual knowledge and split control must be implemented for any instances where key material is stored or managed in clear text.

4.5.6 Key Rotation

Keys must be rotated at defined schedules based on business and system requirements, when there are identified indicators of compromise, or when the knowledge of keys is compromised due to termination of employment.

4.5.7 Certificate Management

All certificates used in the delivery of University services must be issued by an approved certificate authority.

4.5.8 Key Storage

All cryptographic key material used in the protection of High Risk data must be stored within FIPS 2 validated hardware security modules. Access rights must be strictly limited to cryptographic security modules to prevent unauthorized access.

5. Standards and Procedures

Standards and procedures specific to this standard are to be documented and maintained by the individual affiliates 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

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 policy:

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

Revision history of this policy:

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