Effective: *08/08/2022*
Last Revised: *11/18/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Standard Contact:
IT Security Services
security@nebraska.edu

ITS-19: Security of Personally Owned Devices Standard

Standard Contents

1. Purpose

The purpose of the Security for Personally Owned Devices Standard is to define the organization's requirements for enforcing effective security measures to protect University data and information systems when accessed, processed, transmitted, or stored on personally owned endpoints and systems. When conducting University activities, it may at times be necessary for University users to access, process, transmit, or store institutional data on personally owned devices. This Standard serves as a statement of objectives for the protection of institutional and research data as defined in **Executive Memorandum 42.** When institutional data is accessed, transmitted, processed, or stored on personally owned devices users are required to meet their shared obligation and responsibility to secure data by properly self-managing the privacy and security settings on their personally owned device.

2. Scope

This Standard shall apply to all University of Nebraska System ("University") personnel. All users (employees, students, 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 best practices pertaining to the use of personally owned endpoints and systems when accessing University information systems and data. 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 for Personally Owned Devices Standard.

4. Security of Personally Owned Devices

4.1 Use of Personally Owned Devices

4.1.1 Personally Owned Device Security

University personnel are encouraged to maintain safe and secure personal devices with up-to-date software and appropriate security protections to safeguard personal data. University personnel that engage in University business with a non-university device must follow the Policies, Executive Memoranda, Standards, and guidance provided by the University, as well as comply with appropriate safeguards required by state and federal regulations.

Publicly Accessible Medium Risk Information Systems

University personnel may access University information systems that contain medium risk data from a personal device if the system hosting the data is publicly accessible outside of University-managed networks. Medium risk data may not be stored on a personal device that does not meet the appropriate minimum security requirements as defined in the **Configuration Management Standard** and associated Procedures.

University **Executive Memorandum 42** requires specific authorization for storing medium risk institutional data on personally owned devices. The exception process to request such allowance must be approved in advance and in writing by the CISO as defined in **ITS Policy Exception Standard**.

Publicly accessible University Information Systems that contain medium risk data and may be accessed using personal devices include but are not limited to:

- Firefly
- MyBlue, MyRed, MyNCTA, & MavLink
- Learning Management System (Canvas)
- eSignature System
- University email
- Multi-factor Authentication (Duo)

Network Restricted Medium Risk Information Systems
University personnel that access institutional or research data from a University information system that contains medium risk data, and is not publicly accessible, must meet the appropriate minimum security requirements for accessing medium risk systems as defined in the **Configuration Management Standard** and associated Procedures. The minimum security requirements for personally owned devices, also known as BYOD (Bring Your Own Device), will be publicly available on the University website.

University **Executive Memorandum 42** requires specific authorization for storing medium risk institutional data on personally owned devices. The exception process to request such allowance must be approved in advance and in writing by the CISO as defined in **ITS Policy Exception Standard.**

High Risk Data
University **Executive Memorandum 42** requires specific authorization for accessing or storing high risk institutional data on personally owned devices. The exception process to request such allowance must be approved in advance and in writing by the CISO as defined in **ITS Policy Exception Standard.** Exceptions will not be allowed for the storage of high risk data on non-University owned systems, cloud services, or removable storage devices like USB drives, SD cards or similar portable drives and devices without documented security controls via the exception process.

4.1.2 Data Return and Deletion
Personnel shall return and delete institutional data maintained on personally owned devices upon request from the University or when their role or employment or access status changes such that they are no longer an authorized user of the data.

4.1.3 Incident Reporting
Personally owned devices that store medium or high risk institutional data that are lost, stolen, have been subject to unauthorized access, or otherwise compromised must be reported within 24 hours as defined in the **Incident Response Standard**.

4.2 Audit of Personally Owned Devices

4.2.1 Device Inspection
In the course of an incident investigation, the University reserves the right to inspect a personally owned device that stores medium or high risk institutional data. Any access to a personally owned device will be carried out in accordance with **Executive Memorandum 16**, as well as follow other relevant University protocols, and legal or law enforcement requirements.

4.2.2 Response to Document Requests and Production
Records or data maintained by the University or University users may be the subject of document requests (e.g., Freedom of Information Act or Family Educational Rights and Privacy Act) or document production (e.g., warrants, subpoenas, court orders, etc.). University users must produce these records or data (or the devices on which they are stored) upon request of the University.

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	11/18/2022
Approved by:	Bret Blackman	IT CIO	11/18/2022

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published
1.1	11/18/2022	Clarified language in section 4
1.2	01/09/2023	Added Multi-factor Authentication (Duo) to list of services in Publicly Accessible Medium Risk Information Systems in section 4.1.1