WAYNE STATE UNIVERSITY

Computing & Information Technology

Standards for Personal Devices Accessing University Resources

Purpose

This standard establishes the need for the University to institute consistent controls for utilizing personal devices for accessing University resources while on campus and remotely.

Scope

The scope of this policy covers the use of all personal devices that are used to access Wayne State electronic systems.

Roles and Responsibilities

University IT staff will design and deploy information systems that support accessing University resources for both University issued and personal computing devices.

University management will enforce minimum requirements as defined in this document for any employee using personal devices for accessing University data.

The C&IT Information Security office will assist system administrators in ensuring their systems and applications are applying appropriate safeguards for allowing use of personal devices.

Personal Devices, Procedures, and Guidelines

Detailed procedures, standards, and guidelines will be authored and maintained by the C&IT Information Security Office. New or modified procedures, standards and guidelines will be communicated to all University IT staff once approved by the C&IT Risk & Security Oversight Committee.

Organizational Coordination

The C&IT Information Security Office will solicit feedback from on-campus IT units regarding the effectiveness and applicability of this policy and related standards, taking it into consideration during periodic policy review. This policy and associated documents will be openly published and communicated to all IT staff at a minimum of an annual basis.

Compliance

All university units are required comply with this policy and any associated standards. Any exceptions to this policy must be approved by the C&IT Information Security office, will be given a deadline for proper compliance, and will be reviewed on an annual basis.

Standard Review
This standard and any associated procedures, standards, and guidelines will be reviewed at a minimum on an annual basis by the C&IT Risk & Security Oversight Committee.

Definitions

As used in this standard, *"enterprise systems"* are electronic information systems maintained by C&IT that contain institutional data that is defined by the Data governance Committee. Current examples of enterprise systems include Banner, Cognos, and Imaging.
As used in this standard, *"personal devices"* are any computing device that is not issued directly from C&IT or an approved C&IT program. Computing devices obtained outside of an approved C&IT program, even with University funding, may still be considered personal devices. Examples of computing devices are desktops, laptops, tablet, phones, wearables and Internet of Things (IoT).

Most computer accessories such as mice, keyboards, webcams, monitors or desktop printers that have been obtained outside of C&IT programs can be used without restrictions unless the device performs computing or storage of data. For example, enterprise multi-function printers and all-in-one type computer monitors are still considered personal devices if they are not issued by C&IT or an approved C&IT program.

As used in this standard, "two-factor authentication" is a combination of two or more factors 1) something you know 2) something you have 3) something you are.

Personal Device Standards

This standard does not discourage or encourage use of personal devices or dictate when the University should or should not provide computing devices. The intent of the standard is to provide the security controls necessary to protect the confidentiality, integrity and availability of the Wayne State network and enterprise systems when it is deemed necessary to use personal devices.

Wayne State recommends any device that is used to access University systems follow a set of minimum security best practices including use of anti-malware tools, maintaining current software updates and use of strong passwords. These controls may be required for certain activities or certain data classifications. If the controls are not specifically defined in the document the Information Security Standard for Device Configuration should be followed.

Unrestricted personal device use
Many University systems are designed to be publicly accessible via the Internet. Examples of these systems are wayne.edu, Academica and WayneConnect. These resources may still require a Wayne State account and valid credentials to access but do not require any device specific security controls.

Limited restrictions on personal device use
Unless the activity being performed is described elsewhere in this document the following activities can use personal devices with limited restrictions. Some restrictions may apply such as additional steps for two-factor authentication or remotely accessing certain systems.

- Most general activities performed by students and faculty for Academic purposes, for example accessing the University Learning Management System.

- Access from mobile devices such as cell phones or tables that use a C&IT approved mobile application obtained through the manufacturer's official app store, such as Outlook or Wayne State Mobile.
- Attend a virtual presentation when non-public WSU information is presented. As long as the information is presented in read-only fashion where reasonable steps have been taken to prevent the information from being saved, printed or recorded. For example, attendees viewing a PowerPoint presentation given over Zoom or Microsoft Teams when recording is disabled or access to the recording is restricted.

Permitted with Required Security Controls

The following requirements are mandatory for any employee that is directly accessing and Wayne State enterprise system when using a personal device. This includes faculty when performing administrative actives, student employees and interns.

- Devices should adhere to University Secure Computing Standards, at minimum devices must:
    - Be capable of obtaining security updates and keep up-to-date following manufacture recommendation.
    - Use an up-to-date anti-virus/anti-malware software.
    - Be secured with a strong password, passphrase or passcode.
- Devices should not be shared with others. When necessary to use a shared device a separate account must be used that is not accessible by others.
- Enterprise systems may not be directly accessed using kiosk type systems unless approved by the Information Security Office.
- Non-public data must not be stored on personal devices without an approved exception. If an exception is granted data must be stored encrypted by using an approved methodology.
- E-mail regularly containing non-public information may only be accessed through approved apps or via WayneConnect. E-mail forwarding should also be disable when using a personal device when regularly receiving or sending non-public data via e-mail.

Restricted use of personal devices

The following activities must not be performed using personal devices

- Any activity that is explicitly defined by the data owner or University senior leadership.
- Any system administration, application development, or other IT activities that involve enterprise systems unless the personal device is only used to access an approved system for this activity, such as through SSH Proxy, RDP or VDi, and that system has implemented appropriate safeguards to prevent copying, storing, printing or otherwise recording information.
- Any activity that requires accessing or storing administrator or root type credentials to an enterprise system. This includes use of personal accounts that have been given this level of access that might normally be used for lesser restricted activities.

Remote Access

Many applications do not require the user of VPN and may be accessed directly via a web browser or published via Academica. Access to some enterprise applications require a method of secure remote access when not connected to the Wayne State Secure Network.

- All students, faculty, employees and university affiliates may install and use the VPN client on any personal devices that will support the software without any restrictions.

- Applications that are published through Citrix, Microsoft Virtual Desktop or other similar tools that have been approved by the Information Security Office may be used on personal devices.
- Other remote access solutions, such as Direct Access or RDP without the use of VPN are not permitted for personal devices.
- Multi-factor authentication is required for all remote access, including the VPN.

Research
Use of personal devices for research should follow the requirements set forth in the grant or other governing documents of the research project. If such requirements do not exist research staff should follow at least the required security controls. If there is conflict between governing documents and this document the stricter control should be followed.

Non-Compliance
The C&IT Information Security Office may limit access to or from a system if it does not meet the above guidelines.

Exceptions
Exceptions to these standards may be granted by the Information Security Office given business justification and a satisfactory risk assessment. In such cases, the system owner shall acknowledge the risk and take responsibility for any breaches, incidents, or compromises that occur as a result of not utilizing a supported operating system.