M | LSA TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Protect Your Personal Devices

An Resource Guide for U-M Faculty, Staff and Students

Smartphones, tablets, and laptops keep us connected and make us more productive. If you use your devices to teach, learn, research, or work; **especially if you are accessing sensitive U-M academic, research, or administrative data**, the U-M expects you to secure your devices and use them responsibly.

Guidelines for Personal Devices

- □ Review **Secure Your Devices** content from Information & Technology Services to learn how to protect your devices, data, and network connections, as well as tips for working remotely & via videoconference.
- □ Ensure that your **computer** and **mobile devices** are secured in accordance with U-M policy. You are responsible for complying with **SPG 601.07**, **SPG 601.33**, **DS-07**, and **SPG 514.04**.
- □ Ensure your **Windows**, **Mac**, **iOS** or other devices are running the most current Operating Systems. Computers unable to run the most current OS are not generally able to receive OS and software security patches and updates which enable them to be secured to the policies listed above.
- □ Use U-M data storage services which are operated, managed, and secured by U-M IT experts vs. storing it locally on your device. If your **Department permits sensitive data** to be used on personal devices, you are expected to protect data by securing and properly managing these devices to **U-M standards**. Consult the **Sensitive Data Guide** to see which services are appropriate and meet federal, state, and U-M guidelines.
- □ Choose **web browser security settings** that protect your privacy and enhance security.
- □ Follow U-M tips to **Improve** and **Secure** your Home Internet.
- □ Use the **U-M Virtual Private Network (VPN)** to create a secure, encrypted connection between your device and the U-M network.
- □ **Travel** safely with technology and apply appropriate additional steps to protect your device and data when you are using public networks or traveling abroad.
- □ Use **antivirus** software to protect your device (beyond security software that is standard on your Windows or Mac device). Consider personal accounts with vendors such as **Norton** ($40 Standard Account), **McAfee** ($40 Standard Account), or **Malwarebytes** (Free Standard Account) .
- □ Install a pop-up blocker to prevent both nuisance and malicious pop-up windows and inline advertising during web browsing. Consider vendors such as **UBlock Origin** (Free Download).
- □ Practice good **Online Hygiene** to review your digital footprint, protect yourself from **phishing** and other scams and malware, and **report** security incidents, compromised devices, or data breaches promptly.

Summer 2023