Home / Protect Yourself / Secure Your Devices

Protect Your Personal Linux/Unix Computer

If you are permitted to access or maintain sensitive institutional data using your personally owned computer or self-managed university-owned computer, please meet the minimum expectations below.

See Your Responsibility to Protect U-M Data When Using Your Own Devices for a complete list of your responsibilities when using your own devices to work with sensitive U-M data.

By meeting the minimum expectations below, you also protect your personal data.

Hide All Content

Settings

Require a password for access to your computer.

Follow these guidelines for a strong password.

Use a screensaver.

Set your screensaver to activate after 15 or fewer minutes of inactivity, and require your password to unlock it.

Turn on your local firewall.

It is normally turned on by default. Current versions of Linux use the iptables firewall. Standard firewall practice dictates that you deny everything and then allow only services that you require. Consult the documentation for your system to learn how to adjust the firewall rules to ensure that only the services you require are enabled.

Disable root login / su - and implement sudo.

Implementation of sudo will allow privileged access as required and will log all such activity and link specific actions to specific individuals. It also avoids shared root accounts, which can make it more difficult to securely deprovision access for an individual or contain security incidents involving compromised credentials. Many Linux distributions already implement the no root login feature and force the use of sudo. If the distribution you are using does not already support sudo, install the sudo package and configure it appropriately (ensure "su -" does not switch user to root. Consider bash, vi, and other apps that can shell out to root).

Disable or remove guest and defaults accounts.

Best practice is to not allow guest, default, or shared accounts access to the workstation. Verify that there are no suspicious accounts in the /etc/passwd file. Ubuntu has the guest account enabled by default. Edit the /etc/lightdm/lightdm.conf file and add the following line to the end of the file:
allow-guest=false

Install U-M VPN software if you expect to use untrusted networks.

Untrusted networks include guest wireless in a hotel or coffee shop. Members of the U-M community can download and install the U-M VPN or the one appropriate for their campus. See Use a Secure Internet Connection.

Use full disk encryption for laptops.

Full disk encryption will prevent unauthorized access to the sensitive data stored there should the laptop be lost or stolen. Install a version of Linux/Unix that supports full disk encryption.

Use anti-virus software

See Anti-virus for Personal Computers for recommendations and links.

Connections

Use a secure internet connection, such as a wired connection or MWireless.

Learn how to set up MWireless and about secure connections to help keep you and the university protected.

Turn on the appropriate U-M VPN for your campus if using untrusted wireless networks.

Turn on the VPN every time you connect to an untrusted network. (You will need to have it installed on your device first.) See Use a Secure Internet Connection for information about VPNs for the Ann Arbor, Flint, and Dearborn campuses, as well as the U-M Health System.

WiFi and Bluetooth

Turn off optional network connections like WiFi and Bluetooth when you are not using them.

Management

Update your OS.

Turn on automatic updating to keep your Linux/Unix operating system updated.

Update your applications.

Keep your applications updated to take advantage of security updates and other improvements.

Configure audit logging (syslog) to help you to reconstruct a timeline of events or system activity.

This information is important for responding to security incidents or resolving system errors. Audit rules are specified in the file/etc/syslog.conf. Typically, the system stores sequential logs in files located in the /var/log directory.

Configure ntp time synchronization.

Many Internet services rely on the computer's clock being accurate. Also, accurate time/date stamps in logged activity aid any forensics analysis and system troubleshooting. Install the ntp package. Configure the ntp.conf to use the university’s time servers at ntp.itd.umich.edu or set up a cron job using rdate to set the clock every four hours.

Use reputable software providers.

Only install applications from reputable software providers.

Be aware that certain types of sensitive data cannot be accessed or maintained outside the U.S.

Examples of such data types include Export Control, HIPAA, and FISMA. See the Sensitive Data Guide for details.

Before you sell or give away your computer, erase the hard drive securely.

See Prepare Devices for Disposal.

Report security incidents.

If you use your computer to maintain or access sensitive institutional data and it is lost or stolen, notify the ITS Service Center.

Instructions for security settings and tips for protecting your Linux/Unix computer are available from various vendors:

- RedHat security: RedHat's security page
- Keeping Up to Date: Updating RedHat's Fedora Core
- SUSE security: SUSE's security page
- Ubuntu
- Netfilter: Linux firewall

Additional Best Practices

Consider these additional options for enhanced security for your computer and the data maintained on or accessed from it.

- **Back up your data.** Always keep a backup copy of files you do not wish to lose. Hard drives wear out and fail. Devices can be lost or stolen. The university offers several file storage options you can use. Check the Sensitive Data Guide to see which services are appropriate for certain types of sensitive institutional data.

- **Choose web browser security settings** that protect your privacy and enhance security.
- **Be safe online.** Learn about strong passwords, how to protect your identity, how to avoid phishing scams, and more.
- **Put a sticker on your computer** with your name and contact information. This low-tech, practical step enables somebody to contact you if they find your lost computer.
- **Register your devices.** The U-M Police Department offers a free laptop and personal electronics registration program to members of the U-M community to deter theft and assist in the recovery of stolen property.
- **Travel safely with technology.** Take precautions when you are away from home to protect your privacy and the university's sensitive data.
- **Utilize "brute force detection"** by installing DenyHosts or Fail2ban. These tools will monitor your logs for failed remote attempts and prevent brute force password attacks.

U-M Policies and Standards

- Responsible Use of Information Resources (SPG 601.07)
- Security of Personally Owned Devices that Access or Maintain Sensitive Institutional Data (SPG 601.33)
- Unit-Specific Requirements for Self-Management of Personally Owned Devices that Access Sensitive Institutional Data (DS-07)
- Tech Tools: Cell Phones and Portable Electronic Resources (SPG 514.04)