Risk Advisory
Securing Laptops and Mobile Devices

Overview

Stolen laptops are a common cause of unauthorized disclosure and loss of data at universities. If your laptop is lost or stolen, resulting in a breach of personal information, Washington state law (RCW 42.56.590) requires notification within 30 days to anyone impacted by the breach. State law considers the type of personal information and whether it was encrypted in determining if the loss is a breach.

More information, including links to precise definitions (e.g., “personal information”) as well as relevant UW policies may be found below. The best practices listed below will help you secure personal and UW institutional data on laptops and other mobile devices.

Best Practices

1. **Take immediate steps to secure your device when you receive it.**
    - Encrypt it.
    - Protect it with a strong password.
    - Register it with appropriate administrative and/or purchasing staff.
    - Turn on location tracking so you can find it if it is lost or stolen.
    - Create a user profile that is separate from the administrative account and only use the administrator account for administrative tasks.

2. **Keep the operating system (OS), BIOS, and software updated and patched.**
    - Keep the OS and applications updated and patched.
    - Use antivirus software and keep it updated.
    - Delete applications that you are not using, including old versions of software that remain installed after an upgrade.
    - Update the BIOS on PCs as needed. Check with your computer's manufacturer (e.g., Dell) for information on how to update the BIOS.

3. **Secure the data.**
    - Know UW data classifications.
    - Keep data and devices backed up.
    - Delete UW confidential and restricted information from devices.
    - Observe standards for use of HIPAA, FERPA, and other types of protected information if you access, use, or store them.

- Review APS 55.1, Mobile Device Use and Allowance Policy, particularly Section 4, for information about your responsibility for UW data on devices, whether they are personally or UW-owned.

4. **Secure connections.**
   - Use Husky OnNet or another UW VPN service.
   - If using Husky OnNet VPN, understand the difference and when to use the full tunnel (all Internet access) vs. the split tunnel (UW traffic only) options. See "**When you are off-campus, what can you access?**" on the Husky OnNet page.
   - Use eduroam for wireless connections on campus and other institutions worldwide.

5. **Secure connections and devices at home and when traveling.**
   - Enable the firewall on your devices. Default firewall settings are acceptable for Macs and Windows machines, but verify that they are turned on.
   - Use a strong password for users to connect to home routers, and always change the default administrator password. Use separate passwords for user and administrator access. Disable remote administrative access if that feature exists for your home router.
   - Don't allow family members, friends, or roommates to use computers and devices that you use to access UW data and information systems.
   - Consider taking a temporary laptop with you when traveling.
   - Review other considerations for traveling on the Tips for Traveling Risk Advisory.

6. **Protect your device from theft.**
   - Never leave your laptop in a vehicle.
   - Do not leave it unattended, even for a minute.
   - Secure your laptop in an office with cable locks, lockdown devices, or inside a locked drawer. Try not to leave your device in plain sight -- even if locked.

7. **Dispose of devices properly.**
   - Ensure UW data has been deleted if you surplus UW-owned computers or devices or discard, recycle, donate, or sell your personal computer or device.
   - Review the Secure Disposal Risk Advisory to ensure that all data has been deleted.

8. **Report incidents.**
    - Review the "Report an Incident" page so that you are prepared in case an incident should occur.
    - If a device containing University information is lost, stolen, or compromised report the incident to the appropriate delegated authority.
    - If your computer is compromised, you may need to reinstall the operating system. If it is a University-owned device, check with your department's IT staff. For personal computers, consult the UW Computer Vet in Odegaard Library or with your device's manufacturer.

Resources

- **Relevant UW policies, laws, and employee responsibilities**
    - Access and Use Agreement for UW Data and Information Systems https://uwnetid.washington.edu/agree/
    - APS 2.2, UW Privacy Policy
    - APS 2.4, Information Security and Privacy: Roles, Responsibilities, and Definitions
    - APS 2.5, Information Security and Privacy: Incident Reporting and Management
    - APS 2.6, Information Security Controls and Operational Practices
    - APS 55.1, Mobile Device Use and Allowance Policy
    - RCW 42.56.590
- **Mobile Devices online training**