Office of the Chief Information Security Officer
Risk Advisory: Remote Access to UW Information Systems

BACKGROUND

University employees may have the ability to access the University's information systems from computing devices and locations other than their regular workspace or outside the University's network. Remote access puts systems at higher risk of attacks and unauthorized access, which represents a higher risk to the confidentiality, integrity, and availability of University information. The University does not have control over the remote connection or the devices; therefore, additional precautions should be taken by employees when working remotely.

BEST PRACTICES

If you access University information or systems remotely, the Office of the Chief Information Security Officer (CISO) encourages you to consider the following:

Updates

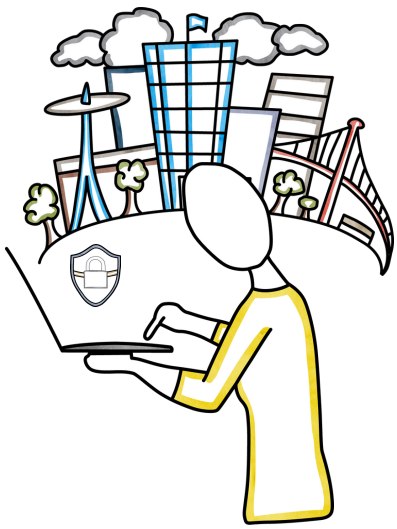
- Keep systems up to date by enabling automatic updates in the operating system and applications.

Passwords

- Protect passwords and consider using a password manager.
- Don't share passwords used to access University information and systems.
- Don't use the "remember my password" feature when accessing University information.

Devices

- Use UW devices and systems when working with UW information whenever possible.
- Lock the screen when away from the computer to prevent unauthorized access.
- Keep others from viewing the screen on devices when accessing University information.
- If you can avoid it, don't store University information on non-UW devices.



Office of the Chief Information Security Officer
Risk Advisory: Remote Access to UW Information Systems

- Delete sensitive UW information that is accidentally downloaded onto personal devices.
- Delete locally saved files on public or shared computers.
- Physically protect devices from theft or inappropriate access.

Secure Connections

- Use anti-virus software and configure it to automatically update.
- Use anti-virus software to scan portable storage devices, e.g., thumb or external hard drives that contain University information.
- Connect to UW desktops via remote desktop connections from personally owned computers.Use eduroam to connect to WiFi on the UW campus and from participating campuses and institutions around the world.
- All faculty, staff, and students can use the Husky onNet VPN Service for connecting to the UW network from remote locations.

Other Considerations

- Use encryption whenever possible when storing University information on portable devices, such as laptops.
- You should not consider your online activity to be private when using public or shared Wi-Fi or computers.
- If a device containing University information is lost, stolen, or compromised report the incident to the appropriate delegated authority.

This list is not exhaustive. Other information security settings may apply to the particular operating system, information system, network, or device you are using.

For additional information, consult your department IT support person or help@uw.edu.

RESOURCES

eduroam

Husky onNet

More Tips from IT Connect

Report an Incident