Information Security Risk Advisory
Remote Access to UW Information Systems

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:

- Use anti-virus software and configure it to automatically update,
- Configure your operating system and applications to automatically update all critical software patches,
- Protect passwords used to access University information; consider using a password manager,
- Don’t share passwords used to access University information,
- Don’t use the “remember my password” feature when accessing University information,
- Use encryption whenever possible when storing University information on portable devices,
- Use anti-virus software to scan portable storage devices, e.g., thumb or external hard drives that contain University information,
- If you can avoid it, don’t store University information on non-UW devices,
- Delete locally saved files on public or shared computers,
- Physically protect devices from theft or inappropriate access,
- Keep others from viewing the screen on devices when accessing University information,
- 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.

Resources

Risk Advisory on Smart Phone Configuration:
http://ciso.uw.edu/resources/risk-advisories/smartphone-configuration/