University of Toronto
Information security remote work guidelines

Our goal is enabling you to work securely wherever you are.

Keeping your data and computing environment safe and secure is a team effort. While the information security team, your information technology (IT) support and our vendors work to protect data, applications, devices and the network, every person in our community has a role to play – especially in a changing, post-pandemic world.

We are most secure when we are Secure Together.

If you work remotely with self-managed devices (home computers, laptops, phones, etc.) and access institutional data, it is your responsibility to secure your devices and use them responsibly.

For devices, at a minimum:

- Use supported versions of operating systems.
- Patch and update the operating system and software/applications with respect to security vulnerabilities.
- Have fully enabled, automatically updating anti-virus software for Windows computers where possible.
- Protect devices with a strong password and/or biometrics.

When working with level 3 and 4 institutional data:

- Enroll in UTORMFA.
- Encrypt data when stored on devices.
- Report to your local IT management and security.response@utoronto.ca any lost, stolen or compromised devices holding University data or enrolled in a university authentication system as a trusted device.
- Use secure connection methods that are encrypted, such as a virtual private network (VPN), secure shell protocol (SSH) and transport layer security (SSL/TLS) to connect to university systems before accessing data.
- Store data on university-managed systems. The University's offering of Office 365 is considered a university-managed system for this purpose. Your department may have others.
- Do not share your devices with people other than those authorized to access the data.

Please contact your local IT team or supervisor if you require assistance.

For more information on how to protect your devices and home network, visit University of Toronto's (U of T) Remote Security Matters web page.

These guidelines have been endorsed by the U of T Information Security Council and approved by the Chief Information Security Officer. This is an evolving landscape, and it will likely change over time. For suggested improvements, please contact security.response@utoronto.ca.