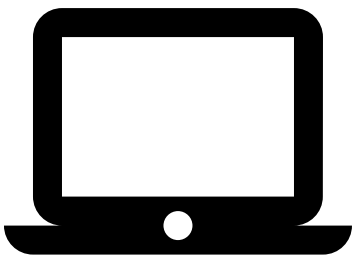
SECURELY WORKING REMOTELY

UND UNIVERSITY OF NORTH DAKOTA
UNIVERSITY INFORMATION TECHNOLOGY

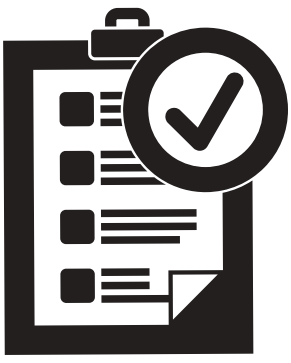
Your Home Network

- Secure your home Wi-Fi network by using a strong username and password
- Only share your Wi-Fi credentials with people you trust
- Do not use public Wi-Fi networks for work related activities
- Use UND provided storage locations (OneDrive or department shared drive)



Using UND Devices

- Abide by the technology policies and standards: Acceptable Use of Technology Policy, Endpoint Security Policy, Data Privacy Policy, Data Classification Standard
- Protect UND owned equipment by using it only for official business
- Do not allow others to use or gain access to UND systems or sensitive data
- If you have a device that needs to be repaired, please contact UIT



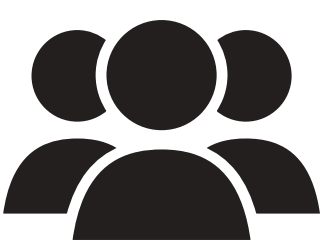
Software Updates

- Keep all your devices up-to-date to avoid security risks
- Only use approved software with your UND owned devices

Data Security

- Do not download or store sensitive data on devices
- Utilize multi-factor authentication (MFA/DUO)
- Utilize UND provided Cisco AnyConnect VPN when accessing non-cloud services (ex: shared drives, Perceptive Content)
- Use Liquid File Secure File Share to send private or restricted information
- Don't print to unattended campus printers
- Look out for Coronavirus (COVID-19) scam and phishing emails and be especially diligent

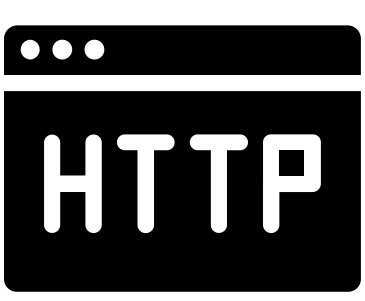
---



Incident Report

- Immediately report any suspected security incidents or suspicious activity to UIT Tech Support

---



Other Resources

- Top Five Steps to Securely Work from Home
- View the Working from Home Cybersecurity Tips training video
- Find out more about how to work remotely on the UIT webpage

SAFEGUARDING UND
UNIVERSITY OF NORTH DAKOTA

701.777.2222