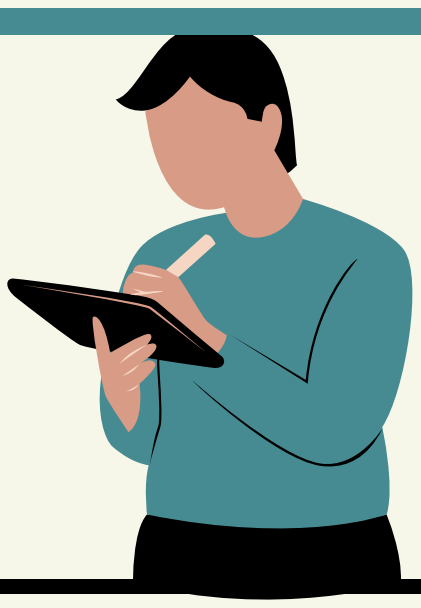
STAY SAFE ONLINE:

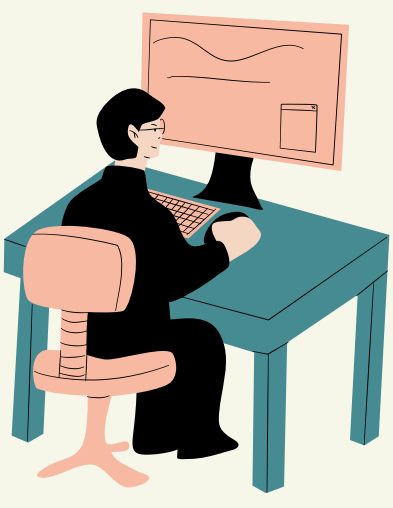
CYBERSECURITY GUIDE FOR PURDUE REMOTE WORKERS

ADHERENCE TO TELEWORK POLICIES



Purdue University has specific telework policies that outline acceptable remote work practices and security measures. Employees should familiarize themselves with these guidelines to understand where and when remote work is permissible, and to adhere to prescribed security protocols.

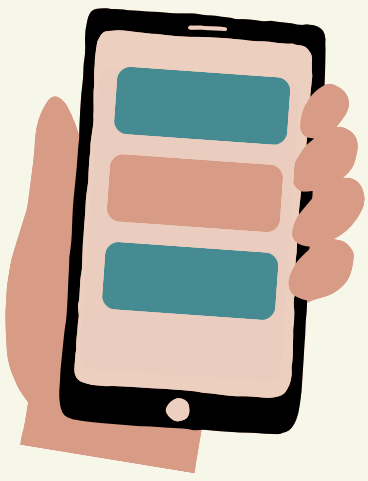
Click here for Purdue's Policy



USE OF APPROVED DEVICES:

It is essential to use only university-approved devices for work-related tasks. Personal devices often lack the necessary security configurations and can expose the university's network to cyber threats. Avoid using personal computers, tablets, and smartphones for professional duties.

SECURE NETWORK CONNECTIONS



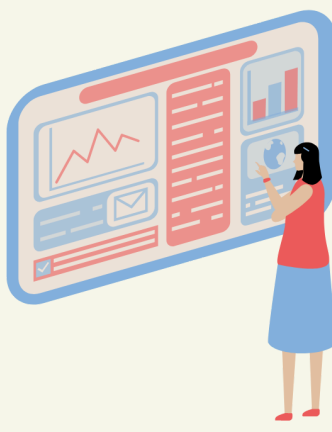
Always use a Virtual Private Network (VPN) when accessing the university's network remotely. A VPN establishes a secure connection by encrypting data, thus safeguarding sensitive information from unauthorized access. Employees should ensure that they connect only to trusted networks or use their cellular network instead of public Wi-Fi hotspots, which are often insecure.

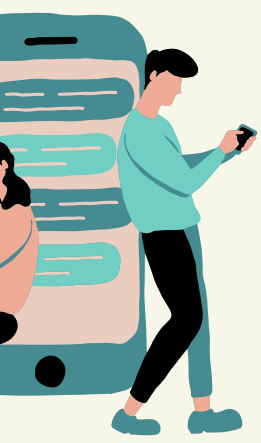
CAUTIOUS ONLINE INTERACTIONS:

Phishing attacks are common cybersecurity threats. Employees should be vigilant and think twice before clicking on links or downloading files from unknown sources. Verify the authenticity of the sender through direct communication if unsure about an email's legitimacy.

DEVICE AND DATA SECURITY:

When working from locations other than home, such as cafes or libraries, never leave devices unattended. Practice securing devices with passwords that are robust—comprising a mix of upper and lowercase letters, numbers, and symbols—and engage multifactor authentication wherever possible to add an additional layer of security.





REGULAR UPDATES AND TECHNICAL SUPPORT:

Keeping software up to date is a key defense against many vulnerabilities. Ensure that all devices and applications are running the latest versions. If technical issues arise, Purdue staff and employees should contact the IT help desk for assistance rather than attempting to resolve problems independently, which can inadvertently lead to breaches in security.

FOR MORE INFO, EMAIL US AT:

cyberaware@purdue.edu