

TELEWORK SAFETY, WORKSPACE AND DATA SECURITY CHECKLIST

Use this checklist as a guide to help you understand the setup of your telework location. As a telework employee, you are responsible to ensure that the designated workspace you are proposing is adequately equipped and complies with these safety guidelines.

Safety Checklist

Location

- Workspace is away from noise, distractions, and is devoted to your work needs
- Workspace accommodates workstation, equipment, and related materials

Electrical

- Sufficient electrical outlets are accessible
- All outlets are covered and in working order (Caution: Do not overload outlets; make sure they can handle the load; If necessary, call your electrician to verify outlet electrical circuit capacity)
- Equipment is fitted with grounding adapters, surge protectors, and overload fuses
- All grounding adapters and power strips/surge protectors that are being used are Underwriters Laboratory approved
- Equipment is placed close to electrical outlets
- Electrical cords/wires are placed so that there are no tripping hazards

Fire Safety

- There is a working smoke detector in the workspace
- A home multi-purpose fire extinguisher, which you know how to use, is readily available
- You have an evacuation plan so you know what to do in the event of a fire

Workspace Checklist

Standard Computer Desk

- Desk surface should be at a height that allows the employee to write without extreme bending over or lifting of the arms and shoulders
- Desk is able to support weight of computer equipment and related support materials

Keyboard

- Keyboard height should allow the employee to type and mouse with arms at 90 degree or greater angle without lifting shoulders and allow for straight wrists; Wrist rest for keyboard and mouse is recommended

Computer Screen

- Screen is about an arm's length from the eyes and tilted back 0 - 20 degrees from user's eyes
- Top of viewing screen is at or below the user's eye level
- Images on screen are sharp, easy to read, and there is no glare on the screen face
- Screen contrast and brightness are adjusted for the best reading of typed characters on screen

Workspace Illumination

- Lighting is not so bright that it causes glare on the screen
- Lighting is not so dim that it causes user to strain when viewing screen
- Screen is located away from the window and/or is perpendicular to window and its plane
- There are no reflections on the screen from windows or overhead lights
- There is no light shining directly into user's eyes
- Task lights are used for source documents and positioned to avoid glare on the screen

Chair

- Chair is fully adjustable, allowing change in height and angle of backrest to provide support to the inward curve of the operator's back and waist (Note: If necessary, use a pillow, rolled towel, or cushion for lower back support)
- Chair is adjusted so that knees are at a 90-degree angle, feet are flat on floor or footrest, and elbows are at the same height as keyboard

Data Security Checklist

Per the policy [Remote Access to IT Resources \(VII.B.4\)](#), prior to accessing IT Resources, remote users must follow must follow the [Remote Access Standards](#), [End User Security Guidelines](#) and any additional guidelines issued by their departmental IT units and/or the owners of the IT Resource(s) to be remotely accessed. The following are requirements for a computer that will be connected to Purdue resources for work purposes.

- All Remote Users whether working from a private (home) or public (coffee shops, restaurants, hotels, etc.) location must use Purdue VPN services
- Access to Purdue IT Resources will be controlled via career account ID and password or two-factor authentication
- At no time will a Remote User provide their password to anyone, including family members; ITaP employees will never ask for a Remote User's password
- All hosts that are connected to the University network must use up-to-date anti-virus software, keep virus definitions up to date, and run regular scans
- Remote Users must ensure that systems used to connect to the University network have the most recent, vendor-supported operating system and application patches applied
- Abide by Data Handling Guidelines for protecting and controlling sensitive or restricted information in hardcopy and/or electronic format
- Mobile computing devices and external storage devices must employ encryption and Purdue information must be stored on a Purdue network share that is backed up

Employee Signature _____ Date _____