Kansas Information Security Office

Teleworking Information Security Guide

This document has been created to help provide employees with information security practices that should be followed when telecommuting. The elements of this guide address information system security, computer security, network security, and physical security. While working at the alternate worksite, employees must follow all organization policies and procedures. Many of these recommendations are from NIST 800-46 Revision 2 "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," and NIST 800-114 Revision 1 "User's Guide to Telework and Bring Your own Device (BYOD) Security." As a telework employee, you are responsible for ensuring that your equipment at the alternate worksite is in proper working order and configured in a secure manner. If you have any questions, please do not hesitate to reach out to the Kansas Information Security Office.

General Security:

1. Know the incident reporting procedures and who to contact if you have a security incident at your alternate work site.
2. Review organization acceptable use and information security policies

Computer Security:

1. Workstation or "Personal" Firewall will be enabled (Typically handled by organization IT)
2. Workstation/Laptop hard drive will be encrypted (Typically handled by organization IT)
3. Workstation/Laptop must be secured when not in use
4. Device must check in with Domain (Work Network) regularly to ensure it is up to date with current policies, updates, and Anti-virus signatures. Notify the service desk immediately if you notice update failures
5. VPN into the state environment as soon as you can, once successfully connected to the alternate site network
6. You must still "lock" your workstation when you step away from it
7. Limit the adding of non-state owned peripheral equipment (printers, scanners, etc.) to your state-owned laptop/workstation unless needed to complete job responsibilities

Network Security:

1. Alternate work site network should segregate the user network from the ISP (Router or Firewall)
2. Default passwords should be changed on routers and firewalls
3. Routers and Firewall should be configured to prevent administration from the internet
4. Updates should be applied to routers and firewalls as available (software and firmware)
5. Alternate worksite wireless networks should be configured to utilize WPA2 with AES encryption for wireless communication
6. The default SSID (Wi-Fi Network Name) should be changed
7. SSID broadcasts should be disabled
8. Disable wireless administration of wireless routers and access points
9. Employees should avoid untrusted networks that are outside of their control or the organization's control (i.e. coffee shops, hotels, etc.)
10. Administrators should limit use of elevated privileges while working from alternate work site

11. It is essential to limit use of any streaming video and Internet browsing on VPN device to reduce bandwidth utilization – excessive use of these will impact efficiency of the VPN connection

Physical Security:

1. When working with restricted-use information, steps should be taken to prevent it from being disclosed to others at the alternate work site location.
2. Paper documents containing restricted-use information should be locked in a container when not being used.
3. Do not place monitors in a location where they may be visible to others (i.e. facing a window)
4. Even though you may be at home, do not write down your passwords

Data Security:

1. Do not store state data locally to the workstation/laptop, leave data on the servers
2. Do not use a portable storage device to take state data back and forth between alternate work site and primary work site
3. Limit the reproduction (printing) of restricted-use information at home if possible
4. If printing of restricted-use information is necessary, create a record of the printout and track from creation to destruction
5. Destroy printouts containing restricted-use information when no longer needed using an appropriate crosscut shredder (Pieces should be 1 mm x 5 mm or smaller).
6. If appropriate destruction tools aren't available at home, securely store data and bring back to workplace for proper destruction when permitted to return.

Resources:

NIST: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

NIST: User's Guide to Telework and Bring Your own Device (BYOD) Security

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

Kansas Information Technology Executive Council: Information Technology Security Standards 7230a

https://ebit.ks.gov/docs/default-source/itec/itec-7230a.pdf?sfvrsn=f3990f07_0