California
DEPARTMENT OF TECHNOLOGY
Office of Information Security

(916) 445-5239
HTTPS://CDT.CA.GOV/SECURITY/

ACCESS CONTROL
INFORMATION SHEET NO. 6
MAY 2017 (REVISED)

Telework Security Considerations

The government workplace is evolving. The ability of state employees to perform official duties from home, field office, or other geographically convenient worksites is increasing the need to examine telecommute, telework, and mobile workforce information and system access arrangements. In addition, California's green initiatives and increasingly constrained fiscal environment encourages the State of California to be more innovative in serving the needs of Californians more efficiently and effectively by leveraging the advances in technology (e.g., mobile computing devices, remote connectivity, wireless voice and electronic communications).

As state agencies consider adopting telework as an alternative to the traditional office environment, it is important to understand the security risks and subsequent mitigation strategies that must be established. This Information Sheet identifies those security considerations; however, it does not address human resource and bargaining unit (BU) issues. For more details on telecommuting work options, including definitions, guidelines, and policies, refer to the State's Telecommuting Advisory Group at http://www.dgs.ca.gov/dgs/ProgramsServices/telework.aspx and the Department of Human Resources Workforce Planning at http://www.calhr.ca.gov/state-hr-professionals/Pages/workforce-planning.aspx. Agencies should also be cognizant of the provisions of the BU contracts applicable to its employees and the laws applicable to the types of information used in the course of the employees work.

The key to establishing a secure telework arrangement with the right security controls is to design the alternative work site and computing environment in the same manner as the primary headquarters (HQ) office location. This means addressing information security (confidentiality, integrity and availability) and information (data) in three states:

- At rest or when it is located in a secondary storage device, such as a hard drive or thumb drive
- In transit between the HQ site and the telework location
- In process, while the employee is using the information

This applies to all types of data used for official business: public, confidential, and/or sensitive. Ensuring the availability of non-confidential data that is critical in the performance of the work is as important as ensuring proper access controls for confidential information.

Agency management must also understand the budgetary trade-offs associated with telework. For example, although traffic congestion and commuting overhead costs may decrease, the cost

of supporting the appropriate technology and the required security measures will almost certainly be greater. Using a *defense in depth* strategy can strengthen a legitimate business need to move operations outside of the normal boundaries. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, has been used as a framework in developing this Information Sheet. Agencies should refer to this document, and the NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, for additional guidance in establishing a secure environment for telework capabilities.

Information Technology (IT) Responsibilities

- Establish and use a securely configured Virtual Privacy Network (VPN) connection between agency headquarters and the telework site. This will help ensure firewalls, encryption and tunneling protocols adequately protect the information while in transit across public networks.
- Equip teleworkers with authorized government-owned and government–issued equipment (e.g., laptop or workstation, thumb or flash drives) and manage those devices as part of the agency assets.
- Establish an internal process so routine system updates and upgrades on anti-virus signatures, security patches, and other optimal configurations can be pushed to the teleworker's computing device automatically by the IT department.
- Use a Network Access Control (NAC) approach, when possible, to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication, and network security enforcement.
- Equip laptops with add-on biometric devices, like a fingerprint reader, for secure access by the designated employee only.
- Use two-factor authentication, such as a combination of strong passwords (*something you know*) and endpoint device authentication (tokens-*something you have*), to guard against unauthorized network access. Manage the token devices as an enterprise asset.
- Enable "session lock" on computers so when employee leave their desks, they go into sleep mode and requires employees to log in using a password to bring their session back up. Do not allow employees the ability to disable this or similar access controls.
- Use full-disk encryption and strong passwords on mobile devices (e.g., laptops, hard drives, thumb drives) so the information cannot be accessed if lost or stolen, and would render it useless to an unauthorized user.
- Configure wireless devices so that they do not automatically attempt to join wireless networks they detect. If wireless is a business requirement, consider third party wireless solutions, like cellular air cards, which are typically more secure.
- Conduct automatic backups to the headquarters' site over the network to protect the information from loss or destruction and enable it to be accessible by other authorized personnel.

Management Responsibilities

- Establish an enterprise telework policy that defines the classifications and types of functions permitted to telework since not all jobs lend themselves to secure telework. For example, it may not be feasible to allow human resources staff to telework, given the sensitive nature of employee information they handle on a daily basis. In some cases, legal or state policy requirements may specifically prohibit the electronic or physical; removal of such material from HQ or the traditional workplace environment (e.g., certain employee personnel records are to be "adequately protected and shall not leave the premises". See State Administrative Manual section 8534).

- Establish and routinely review all telework agreements to ensure they are in compliance with the agency's information security and privacy policies.
- Work with employees to ensure they fully understand the security ramifications and have the knowledge to comply with the security and privacy requirements including:
    - Ensuring employees receive information security and privacy training on an annual basis.
    - Ensuring the employee has acknowledged receipt of the state agency's Acceptable Use Policy, and monitoring employee usage for conformance.
    - Informing employees of their responsibility in making immediate notification the agency's Information Security Officer should a breach or loss of data occurs.
- Monitor and enforce employee conformance with acceptable use, and security and privacy requirements.
- Develop secure methods for the protection of sensitive paper documents and other materials that contain confidential information, such as personal information.
- Establish procedures for tracking the removal and return of potentially sensitive materials, when such removal is authorized.
- Ensure all equipment is collected and accounts are disabled and removed when the employee leaves the organization or modified as appropriate when employee transfers to another program area.
- Ensure all equipment is re-imaged or wiped to remove data when the employee leaves the organization or transfers to another program area.
- Follow normal equipment disposal practices at end-of-life.

Teleworker Responsibilities

- Ensure the home telework environment is equipped for adherence to security and privacy requirements.
- Report security incidents immediately to the agency's Information Security Officer.
- Participate in the agency's annual information security and privacy training.
- Achieve sufficient technical proficiency to implement the required security measures.
- Provide a high level of security to any personal or private information (paper or electronic) accessed at the telework site or transported between locations. For example, do not allow family members or others to use the work-issued equipment or computer access, and secure all confidential, personal or sensitive material in a locked file cabinet when not in use, or when visitors are present.
- Comply with agency policies such as the Acceptable Use Policy and any additional requirements identified in the telework agreement.
- Remain sensitive to individual rights to personal privacy.
- Equipment and work papers should be moved from the vehicle to the alternate worksite and not be stored in the vehicle even overnight.

Resources

- NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access* - http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems*
- *and Organizations* - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security* - http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

- U.S. Office of Personnel Management, *Guide to Telework in the Federal Government* – https://www.telework.gov/guidance-legislation/telework-guidance/telework-guide/guide-to-telework-in-the-federal-government.pdf
- Telework.gov - https://www.telework.gov/
- Department of General Services Statewide Telework- http://www.dgs.ca.gov/dgs/ProgramsServices/telework.aspx
- Department of Human Resources Statewide Workforce Planning - http://www.calhr.ca.gov/state-hr-professionals/Pages/workforce-planning.aspx