

REMOTE COMPUTING POLICY

IS Team Approval: Unanimous, April 14, 2005

TAB Review Date: April 18, 2005

TAB Approval Date: May 16, 2005

Director Approval Date: December 19, 2005

OSF Specification:

7.8 Remote Computing

Remote computing uses communications technology to enable staff or agencies to work remotely from a fixed location outside of their organization. Suitable protection of the remote computing site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. It is important that remote computing is both authorized and controlled by management and that suitable arrangements are in place for this way of working.

Procedures must be developed from best practices to authorize and control remote computing activities. Agencies should only authorize remote computing activities if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the agency's security procedures. The following should be considered:

- A. the existing physical security of the remote computing site, taking into account the physical security of the building and the local environment,
- B. the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system, and
- C. the threat of unauthorized access to information or resources from other people using the accommodation.

The controls and arrangements to be considered include:

- A. the provision of suitable equipment and storage furniture for the remote computing activities,
- B. a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the user is authorized to access,
- C. the provision of suitable communication equipment, including methods for securing remote access,
- D. physical security,
- E. the provision of hardware and software support and maintenance,
- F. the procedures for back-up and business continuity, and
- G. audit and security monitoring.

ODCTE Implementation:

ODCTE provides VPN (Virtual Private Network) connections to allow agency employees to work from remote locations. Such locations may include, but are not limited to, an employee's home, hotels, or conference centers. VPN connections allow direct connection into the ODCTE network, and therefore must be properly secured. Such security must include:

A. Access control

1. It is the responsibility of the user to ensure unauthorized persons do not use the VPN connection, and that any agency data on the device is secured.
2. SDCS will install an approved firewall on a mobile device that is capable of being attached to a network.
3. It is the employee's responsibility to keep the firewall up to date.
4. Passwords must meet the agency password management policy.

B. Backups

1. It is the responsibility of the user to ensure agency data on the device is backed up appropriately.
2. Whenever possible, agency data should be copied to the ODCTE network so the data may be protected by the network backup.

C. Virus protection

1. It is the responsibility of the user to ensure that the virus protection is updated on a regular basis.
2. The software must be updated and antivirus scanning performed on a weekly basis.

D. Spyware/malware

1. It is the responsibility of the user to ensure that all computers used for VPN access to ODCTEs network are free of spyware and malware.
2. Appropriate antispyware software must be installed, run and updated regularly.

For assistance with this policy, please contact Computer Support.