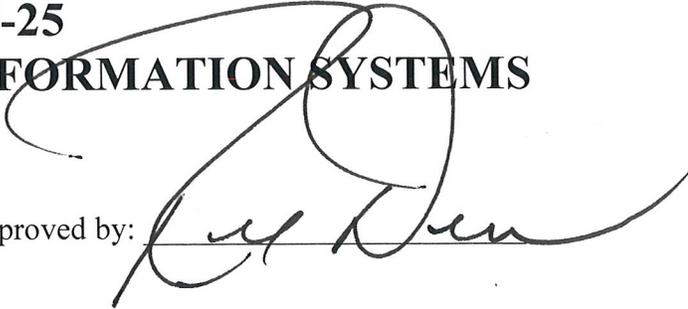




POLICY 15-25

REMOTE ACCESS OF INFORMATION SYSTEMS

Effective Date: 3/9/2010

Approved by: 

See Also/Cancel: Policy 15-25 (03-07-2008)

POL 15-25 Remote Access of Information Systems

As a state agency we are charged with ensuring that publicly purchased equipment and services are properly utilized and not misused. It is the intent of this policy to set guidelines for remote access that are clear, concise, and can be followed by all staff regardless of employment designation or classification.

1. Purpose

The purpose of this policy is to:

- A. Establish guidelines for implementation of remote access to Washington State Parks & Recreation Commission (Parks) information systems. Remote access is the act of accessing internal network resources from an external location.
- B. Identify the permissible and prohibited uses of such access.
- C. Inform employees, supervisors, and managers of their obligations and responsibilities.
- D. Minimize the potential exposure to Parks, and Parks employees, from damages which may result from unauthorized use of Parks resources.

A copy of this policy is available on the agency N: drive, in the Policies and Procedures section, and supervisors will ensure a hard copy is available upon request from any agency employee.

2. Applicability

This policy is applicable to all employees of the Washington State Parks & Recreation Commission. This includes full-time, part-time, temporary, project and Washington Conservation Corps. individuals. Managers and supervisors are not authorized to make exceptions to this policy unless specifically authorized herein. This policy is directive in nature. Failure to comply with its provisions may result in, but is not limited to, the following: loss of access to all automated information systems, corrective and/or disciplinary action, up to and including dismissal, and/or criminal prosecution.

3. **Requests for Remote Access**

Employees shall make requests for remote access directly to their respective supervisors. Parks will consider each request in relation to the agency's operating, business and customer needs. The supervisor will recommend approval or disapproval of the request. Before recommending approval, the supervisor will determine the type of remote access available and appropriate for the employee's work situation. The recommendation for approval should include the agreed upon remote access method(s). In addition, all recommendations for disapproval shall include the reason for the denial. The supervisor shall forward the request and the supervisor's recommendation through the chain of command to the Executive Leadership Team member or designee, who is the final approval authority for each employee's remote access request.

Access to telecommute must be authorized prior to any employee receiving IPsec VPN remote access to Parks information systems. Each requesting employee must have a valid, signed P-086 Telecommuting Application and Agreement Form on file in the Human Resources Office.

4. **Determination of Remote Access Method**

Remote access provides a secure means for employees to access Parks internal network resources. Currently, Parks offers the following types of remote access depending on the requirements of the employee to use remote access:

- A. IPsec Virtual Private Network (IPsec VPN)
 - i. Requires client software installation and SecurID token subscription
 - ii. Requires current M-003 Internet Access & Email Account Agreement
 - iii. Requires current M-017 Remote Access Application and Agreement
 - iv. Requires current P-086 Telecommuting Application and Agreement

- B. Outlook Web Access (OWA)
 - i. Requires current M-003 Internet Access & Email Account Agreement

- C. Inside Parks Intranet
 - i. Requires current M-003 Internet Access & Email Account Agreement

Supervisors should determine the most appropriate method for remote access. If supervisors need assistance in determining the appropriate method of remote access, they should contact the Information Management (IM) Helpdesk.

5. Remote Access Equipment Attached to the Network

Remote access utilizing IPSec VPN shall only be authorized through the use of state-owned equipment, which includes hardware and software (including but not limited to, personal computers (PC) and laptops).

All equipment attached to the network will be approved by the IM Administrator. The use of personal equipment on agency systems is strictly prohibited. Parks IM does not provide support for any non state-owned property.

Managers and Supervisors are responsible for the assignment, inventory, installation and maintenance of Parks property that is used off-site for remote access by an employee.

6. Software

All software used on agency computers must be licensed and authorized by the IM Administrator. No software, unless specifically approved for use by the IM Administrator, shall be loaded to a workstation or server attached to the network. Public domain and shareware software will only be installed as approved by the appropriate IM staff.

7. Virus Protection

All equipment attached to the network will have an agency licensed anti-virus software program with current virus data files installed and operational. Employees should anticipate regular updates of virus software being automatically downloaded to any computer attached to the network.

8. Responsibilities

A. Employees are responsible for:

- i. Ensuring that all Parks property is used consistent with Policy/Procedure 70-15 Employee Conduct and Ethics.
- ii. Protecting all Parks property from damage, theft, unauthorized or misuse by another. Employees shall keep all Parks property in a secure location and shall take all reasonable steps to ensure that unauthorized persons do not access Parks computer networks, email, or Parks-supported computing environments. This includes use of Parks property when traveling on official business.
- iii. Employees shall not leave Parks equipment unattended while not locked up, whether the equipment is on or off, connected or disconnected to the Parks computer network.

- iv. The equipment shall be password protected to ensure that unauthorized persons cannot access data maintained either on the computer hard drive or accessible through remote access.
- v. Employees are responsible for ensuring that any restricted data or confidential materials remotely accessed are appropriately used and protected in accordance with law and Parks policies, in the same manner as if accessed at the Parks office. This includes the required logon information for all access methods.
- vi. Refusing to grant unauthorized personnel access to agency networks/resources/computers; and
- vii. Reporting any observed or suspected misuse of computer resources through the appropriate chain of command.

B. Managers and supervisors are responsible for providing appropriate oversight and establishing procedures as necessary within their respective program so that:

- i. Employees read, understand and comply with this policy.
- ii. First line supervisors require employee compliance, report misuse, and recommend appropriate corrective or disciplinary action.
- iii. Supervisors must pre-approve, in writing, overtime eligible employees for the use of remote access to department information systems outside their normal duty hours. Remotely accessing department information systems, including OWA, is considered work time.
- iv. Overtime eligible employees who access department information systems during their non-duty hours without supervisor written pre-approval may be subject to corrective action and/or discipline, up to and including dismissal, for violation of this policy.

9. **Permissible and Prohibited Use**

Remote access of agency information systems is provided to send, receive, access, use and store information in connection with official agency business. Unless specifically provided by this policy, public law, ethics guidance letters and/or government regulation, all other use is prohibited.

A. Permissible uses – under limited circumstances.

- i. Remote access of agency information systems will be used for the conduct of official government business and authorized purposes only.

B. Prohibited uses – the agency does not authorize personal use of technologies that remotely access agency information systems including the following:

- i. any use for the purpose of conducting an outside business or private employment;
- ii. any use for any political purpose;

- iii. sending or forwarding virus warnings of any sort to anyone other than IM support staff;
- iv. playing games, streaming video or music/radio stations on or over the Internet unless directly associated with the employee's duties;
- v. subscribing to mailing lists and broadcast services that are not work-related;
- vi. browsing Internet sites or receiving, sending, forwarding, or generating information; of a sexual nature; or that promotes or constitutes discrimination on the basis of race, color, sex, religion, creed, age, marital status, national origin, sexual orientation, disability or veteran status; or that infringes any copyright;
- vii. browsing internet sites whose contents are of a subversive or anti-government nature unless authorized, in writing, by the individual's supervisory chain and the IM Administrator, as part of official duties;
- viii. sending or forwarding unsolicited electronic mail or attachments of a political nature, including lobbying for support of a specific piece of legislation other than as a part of your official department business;
- ix. use of any hacker tools or techniques;
- x. any use for the purpose of supporting, promoting the interests of, or soliciting for an outside organization or group; and
- xi. any use related to conduct that is prohibited by federal or state law, rule or agency policy.

10. Treatment of Confidential/Sensitive Information

Employees may access confidential or sensitive information while using remote access under the following conditions:

- A. Employees agree to hold all such confidential or sensitive information in strictest confidence in the same manner as if accessed from their Parks office and shall not use any confidential or sensitive information for any purpose other than as required by Parks.
- B. Except for internal use at Parks, in furtherance of a legitimate and authorized agency-related business purpose, employees agree not to collect, store, or distribute any confidential or sensitive information collected or derived from using of the remote access service.
- C. Employees agree to implement whatever safeguard is necessary to prevent unauthorized access to confidential or sensitive information.
- D. Upon termination of the remote access, the employee shall ensure that all information and equipment within the employee's possession is immediately returned to Parks.

For purposes of this policy, confidential information shall mean all information exempt from disclosure under state law, and sensitive information shall mean discloseable information that Parks deems sensitive in nature and merits limited access. If an

employee is unsure as to whether information is confidential, the employee should contact the Parks Records Officer.

11. Monitoring

The employee's use of agency remote access technologies to information systems constitutes the employee's consent to lawful monitoring of such use. Monitoring may be done to verify that computers, remote access devices, network and Internet access are used for their intended official permissible uses, and not used for prohibited purposes. Lawful monitoring may include active and passive measures with no expectation of privacy in order to check for authorized use, operational security and protection against unauthorized access by foreign agents or other individuals/groups.

Any employee issued agency computing equipment may be subject to discipline, up to and including dismissal, if the equipment issued to him or her is used in violation of this policy – regardless of whether the employee him or herself is the user.

Unauthorized use of the remote access technologies and evidence of unauthorized use collected during monitoring may subject the user to possible administrative, criminal and/or other disciplinary action, up to and including dismissal.

12. Termination of Remote Access

A. Termination by Employee

An employee may terminate remote access at any time. The employee shall notify his or her supervisor prior to the termination date. Employee and supervisor shall complete the required termination forms and return any state-owned equipment, including the SecurID token.

B. Termination by Employer

An employee's supervisor may terminate remote access if the supervisor concludes that such termination is in the best interest of Parks. Additional reasons a supervisor may terminate remote access include but are not limited to:

- i. The employee has violated a provision of this policy, or policies referenced herein;
- ii. The employee's job or the unit operations are no longer conducive to a remote access arrangement; or
- iii. The employee's job performance no longer meets the expected standards.

Parks shall have the authority to block employee's remote access, in whole or in part, at any time, for any reason, whether or not the access is officially terminated.

Whether the employee or supervisor initiates the termination of the remote access, the employee shall:

- A. Return all Parks property on the first day after the access is terminated
- B. Submit an updated M-017 Remote Access Application & Agreement

13. References

- A. WAC 292-110-010 Use of State Resources
- B. Policy/Procedure 70-15 Employee Conduct and Ethics
- C. Policy/Procedure 70-29 Telecommuting
- D. Policy/Procedure 70-37 Using Electronic Mail
- E. Policy/Procedure 70-38 Internet Connectivity and Use
- F. M-003 Internet Access & Email Account Agreement
 - i. Must have a signed copy on file with supervisor and IM
 - ii. Required for all methods of remote access
- G. M-017 Remote Access Application and Agreement Form
 - i. Instructions included on form
 - ii. Must have a signed copy on file with supervisor and IM
 - iii. Required for VPN access only
- H. P-086 Telecommuting Application and Agreement Form
 - i. Must have a signed copy on file with supervisor, HR, and IM
 - ii. Required for VPN access only