**Policy 6.3.1**

**Remote Access**

**Contact:** Enterprise Security Services Manager

### 6.3.1.1 Purpose

The purpose of this policy is to:

- Adopt procedures for the implementation of remote access, which is the act of accessing internal network resources from an external network location.
- Inform employees of their obligations and responsibilities when using remote access, which are designed to minimize the potential exposure to WaTech/CTS from damages which may result from unauthorized use of WaTech/CTS resources.
- Inform employees of their responsibilities with respect to administering remote access to a third party (i.e., any non-WaTech/CTS employee).

Washington Technology Solutions (WaTech) refers to the “consolidated technology services (CTS) agency” identified in RCW 43.105.

### 6.3.1.2 Procedure for Employee Requests for Remote Access

Employees shall make requests for remote access directly to their respective supervisors. WaTech/CTS 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 this recommendation. The supervisor shall forward the request and the supervisor's recommendation through the chain of command to the Appointing Authority, who is the final approval authority for each employee's remote access request.

### 6.3.1.3 Employee Remote Access Agreement

Prior to an employee being authorized to begin remote access service, the employee must complete and sign the WaTech/CTS Remote Access Agreement. The Remote Access Agreement shall include the method the employee will use to access WaTech/CTS Local Area Network (LAN), email, or WaTech/CTS-supported computing environments. By executing the Remote Access Agreement, the employee is affirming that he or she has read the Remote Access Policy, understands the requirements and prohibitions and agrees to abide by these conditions. After approving a Remote Access Agreement, the supervisor will have LAN Services notified via a Servicedesk request.

### 6.3.1.4 Determination of Remote Access Method
Remote access provides a secure means for employees to access WaTech/CTS internal network resources. Currently, WaTech/CTS authorizes the following types of remote access depending on the requirements of the employee or third party authorized to use remote access:

1. IPSec VPN (requires client software)
2. SSL VPN, (clientless access)
3. Outlook Web Access (OWA)
4. Host on Demand (HOD)

No other remote access method is offered.

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 LAN Services.

### 6.3.1.5 Remote Access Equipment

#### State-Owned

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), laptops, personal digital assistants (PDA), cell phones, and tablet PCs). Remote access from state-owned equipment may also be performed using the SSL VPN service.

Cost center managers are responsible for the assignment, inventory, installation and maintenance of WaTech/CTS property that is used off-site for remote access by an employee.

The employee shall complete the Employee Offsite Equipment Justification form and shall submit the form to his or her cost center manager. Before approving the form, the cost center manager shall ensure that all required equipment is listed. No equipment will be issued until the employee receives the cost center manager's written approval. All equipment provided shall be listed on the Employee Off-site Equipment/Software Inventory form, which shall be completed by employee, signed by both the employee and the cost center manager, and submitted to the Finance Office. All WaTech/CTS property is to be returned to the cost center manager at the termination of the Remote Access Agreement.

#### Non State-Owned

Employees using non state-owned equipment may be authorized for remote access only using SSL VPN, OWA or, HOD. Equipment includes hardware and software, including but not limited to, personal computers (PC), laptops, personal digital assistants (PDA), cell phones, and tablet PCs.

For employees who require remote access to only access their email folders and have access to a non state-owned computer with a suitable Internet browser, the employee may use OWA and shall complete only the Remote Access Agreement. For employees who require remote access to only access IBM mainframes and have access to a non state-owned computer, the employee may use HOD. No state-owned equipment is required.
Access available to internal resources via SSL VPN is dependent upon endpoint inspection of the host workstation. Hosts found to be of limited trust will receive limited access.

While not required, the employee is encouraged to utilize an anti-virus product and (if using DSL or cable) a firewall product on their personal computer as a security best practice. WaTech/CTS LAN Services does not provide support for any non state-owned property.

Employees who have been approved to utilize the non-state owned equipment described above, are on notice that once a work related record exists, such records are public records and are subject to the same retention and destruction schedules as records are referenced in the Records Management Policy. Such records may also be subject to public disclosure. Public records include work related records saved on employee's personal computers, email systems, or other personal electronic devices.

**Wireless Fidelity (WI-FI)**

Use of any WI-FI to access WaTech/CTS-supported computing environments from a private residence must use a hardware firewall recommended by LAN Services. WaTech/CTS employees may request configuration assistance through LAN Services.

On the road, hosted WI-FI services (hot spots) do not require the LAN Services' approved hardware firewall. However, these networks should be treated as an untrusted networks and be used sparingly and only for the duration necessary to complete State business activity. Upon conclusion of business, the wireless adapter should be immediately disabled.

### 6.3.1.6 Employee Responsibilities

Employees are responsible for:

- Ensuring that all WaTech/CTS property is used consistent with [WaTech/CTS Policy 1.1.4 Use of State Resources](#).
- Protecting all WaTech/CTS property from damage, theft, unauthorized or misuse by another. Employees shall keep all WaTech/CTS property in a secure location and shall take all reasonable steps to ensure that unauthorized persons do not access WaTech/CTS Local Area Network (LAN), email, or WaTech/CTS-supported computing environments. This includes use of WaTech/CTS property when traveling on official business. Employees shall not leave WaTech/CTS equipment unattended while not locked up, whether the equipment is on or off, connected or disconnected to the WaTech/CTS LAN.
- 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. The password should comply with the ISB Information Technology Security Standards that requires, at a minimum, an eight-digit password using a combination of at least one special character, capital letter and numeric digit.
- IPSec and SSL VPN service remote access requests will use two-factor authentication from a WaTech/CTS provided hardware or software token device.
- Employees agree to comply with the terms and conditions of all end user license agreements accompanying any hardware, software, SecurID token (utilized if employees are provided VPN), etc. distributed in connection with the remote access service.
Employees are responsible for ensuring that any restricted data or confidential materials remotely accessed are appropriately used and protected in accordance with law and WaTech/CTS policies, in the same manner as if accessed at the WaTech/CTS office. This includes the required logon information for all access methods.

### 6.3.1.7 Prohibited Use

Employees who have remote access shall not use either remote access or WaTech/CTS property for any of the following prohibited uses, including but not limited to:

1. Any unlawful purpose, including transmission of any content that is sexually explicit, libelous, invasive of privacy rights, or advocates violence, bigotry, or bias based on race, color, religion, ancestry, national origin, gender sexual orientation, or physical or mental disability;

2. Accessing any data and/or networks to which the employee does not have prior authorization to access;

3. Altering, tampering, or otherwise modifying the remote access service, or the WaTech/CTS equipment used to provide the remote access service; especially if this tampering is intended to provide dual homing or split-tunneling.

4. Providing access to the remote access service for another person, not an authorized WaTech/CTS employee;

5. Use of the remote access service for means other than performing a purpose related to WaTech/CTS' business or the employee's official duties;

6. Modify, publish, transmit, transfer or sell, reproduce, create derivative works from, distribute, perform, link, display or in any way exploit any content from any WaTech/CTS database;

7. Use or attempted use of the remote access service after termination of the Remote Access Agreement; Upload, post, email, otherwise transmit, or post links to any material that contains software viruses, worms, Trojan horses, time bombs, trap doors or any other computer code, files or programs or repetitive requests for information designed to interrupt, destroy or limit the functionality of any WaTech/CTS computer software or hardware, telecommunications equipment, or WaTech/CTS data or to diminish the quality of, interfere with the performance of, or impair the functionality of the remote access service; or

8. Use of the remote access service to connect a LAN or other network to the State network.

### 6.3.1.8 Treatment of Confidential/Sensitive Information

Employees may access confidential or sensitive information while using remote access. Employees agree to hold all such confidential or sensitive information in strictest confidence in the same manner as if accessed from their WaTech/CTS office and shall not use any confidential or sensitive information for any purpose other than as required by WaTech/CTS. Except for its own internal use in carrying out a legitimate agency-related business purpose, employees agree not to collect, store, sell or distribute any confidential or sensitive information collected or derived from its use of the remote access service. Employees agree to implement whatever safeguard is necessary to prevent unauthorized access to confidential or sensitive information. Upon termination of the Remote Access Agreement, the
employee shall ensure that all confidential or sensitive information has either been destroyed or returned to WaTech/CTS. 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 WaTech/CTS deems sensitive in nature and merits limited access. If an employee is unsure as to whether information is confidential, the employee should contact the WaTech/CTS Public Disclosure Office.

6.3.1.9 Termination of Remote Access Agreement

Termination by Employee

An employee may terminate a Remote Access Agreement at any time. The employee shall notify his or her supervisor prior to the termination date.

Termination by Employer

An employee's supervisor may terminate a Remote Access Agreement if the supervisor concludes that such termination is in the best interest of WaTech/CTS. Additional reasons a supervisor may terminate a Remote Access Agreement include but are not limited to:

1. The employee has violated a provision of the Remote Access Agreement;
2. The employee’s job or the unit operations are no longer conducive to a remote access arrangement; or
3. The employee’s job performance no longer meets the expected standards.

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

Whether the employee or supervisor initiates the termination of the Remote Access Agreement, the employee shall return all WaTech/CTS property on the first day after the Agreement is terminated. Return of WaTech/CTS property shall be documented on the Employee Offsite Equipment/Software Inventory Return form.

6.3.1.10 Third Party Remote Access

Third party requests for remote access shall be directed to the WaTech/CTS Delegated Authority, or designee, responsible for the third party (hereafter “WaTech/CTS Sponsor”). That WaTech/CTS Sponsor will work with WaTech/CTS LAN Services to determine the required remote access method, if any, keeping in mind the additional security risks that third party remote access may incur. Equipment includes hardware and software [including but not limited to, personal computers (PC), laptops, personal digital assistants (PDA), cell phones, and tablet PCs].

The WaTech/CTS Sponsor must, prior to authorizing a third party to begin remote access service, require the third party to complete and sign the Use of State Resources Agreement and corresponding Equipment Check Out/Return form. This agreement and the remote access method recommendation (determined by talking to LAN Services) shall be routed through the chain of command to the Appointing Authority, who is the final approval authority for the remote access request. WaTech/CTS will make a determination, at its sole discretion, based on the agency’s security, operating, business, and customer needs.
The signed agreement and the third party's original Equipment Check Out/Return form must be filed with the divisional contracts office, and a copy of the Check Out/Return form must be sent to the Finance Office. After approving the third party Use of State Resources Agreement, the WaTech/CTS Sponsor will have LAN Services notified via a Servicedesk request.

State-Owned Equipment

Third parties must use state-owned equipment to connect to the State Governmental Network ("SGN") if using the IPSec VPN service for remote access. Cost center managers are responsible for the assignment, inventory, installation and maintenance of WaTech/CTS property that is used off-site for remote access by a third party. Before approving an inventory form, the cost center manager shall ensure that all required equipment or software is listed on the third party's Equipment Check Out/Return form. No equipment will be issued until the cost center manager gives written approval.

The use of state-owned equipment is mandatory for use with the IPSec VPN service, but optional with the SSL VPN service.

Non State-Owned Equipment

Third Parties using non state-owned equipment may be authorized for remote access only using the SSL VPN service, OWA, or HOD. Other connections via non state-owned resources are only allowed at WaTech/CTS' sole discretion. Requests must be made to LAN Services through the WaTech/CTS Sponsor.

Access available to internal resources via SSL VPN is dependent upon endpoint inspection of the host workstation. Hosts found to be of limited trust will receive limited access.

Termination

WaTech/CTS may terminate the third party's remote access if it is determined that termination is in the best interest of WaTech/CTS and in accordance with the contract terms, if any, regarding remote access. The WaTech/CTS Sponsor is accountable for ensuring that all state-owned property is returned to the cost center manager. Return of WaTech/CTS property shall be documented on the original third party's Equipment Check Out/Return form kept in the divisional contracts office, signed off, and routed to the Finance office.

References

- WaTech/CTS Policy 1.1.4 - Use of State Resources
- WaTech/CTS Policy 4.2.2 - Customer or Master Services Agreements and Terms of Use or SLA
- Employee Offsite Equipment Justification form
- Employee Offsite Equipment/Software Inventory form
- Employee Offsite Equipment/Software Inventory Return form
- Employee Remote Access Agreement
- Third Party (Contractor) Use of State Resources Agreement
- Third Party (Contractor) Equipment Check Out/Return form
Procedure 6.3.1

Remote Access

Employee Remote Access

<table>
<thead>
<tr>
<th>Action by</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Discuss with supervisor the remote access request and possible methods of remote access. Submit the request by completing and signing the online WaTech/CTS Remote Access Agreement. If requesting use of state Equipment, turn in a signed Employee Offsite Equipment Justification Form to your cost center manager.</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Work with LAN Services to determine the type of remote access available and appropriate for the employee's work situation. Recommend approval or disapproval of the employee's request using the online WaTech/CTS Remote Access Agreement request process. If approved, forward the request and the supervisor's recommendation through the chain of command to the Appointing Authority. If the request involves state Equipment to be used offsite, consider whether to sign the Employee Offsite Equipment Justification Form. If signed, send a copy to the Human Resources office. Once approved, have LAN Services notified via a PC Help request. Fill out and send the Employee Offsite Equipment/Software Inventory Form to the Finance Office. Upon termination of remote access, fill out and send the Employee Offsite Equipment/Software Inventory Return Form to the Finance Office.</td>
</tr>
<tr>
<td>Appointing Authority</td>
<td>Exercise final approval authority for each employee's remote access request.</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Keep the employee's remote access agreement and, if applicable, the Employee Offsite Equipment Justification form on file.</td>
</tr>
<tr>
<td>Finance</td>
<td>Keep copy of the Employee Offsite Equipment/Software Inventory and Inventory Return forms on file.</td>
</tr>
</tbody>
</table>

Third Party Remote Access

<table>
<thead>
<tr>
<th>Action by</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party</td>
<td>Discuss with the WaTech/CTS Sponsor while working with WaTech/CTS his/her remote access request and possible methods of remote access.</td>
</tr>
</tbody>
</table>
Work with LAN Services to determine the type of remote access available and appropriate for the third party, if any. Recommend approval or disapproval of the request. If approved, work with your divisional contracts office to have the third party complete and sign the third party's Use of State Resources Agreement. Route it through the chain of command to the Appointing Authority for signature.

Once signed, have LAN Services notified via a PC Help request. Fill out and send a copy of the Equipment Check Out/Return form and the signed agreement to your divisional contracts office. Send the original Equipment Check Out/Return form to the Finance Office.

Upon termination of remote access, fill out the copy Equipment Check Out/Return form in the contract file and send to the Finance Office.

Exercise final approval authority for the remote access request.

If necessary, assist with completion of the third party's Use of State Resources Agreement. File the agreement and a copy of the third party's Equipment Check Out/Return form for the duration of the performance.

Keep the third party's original Equipment Check Out/Return forms on file.

Revised: September 1, 2010
Revised: February 6, 2008
Revised: July 29, 2004
Effective and Posted: November 18, 2002