

---

# Virtual Private Networks (VPN) Connectivity and Management Policy

---

## VPN Policy for Connectivity into the State of Idaho's Wide Area Network (WAN)



**02 September 2005, v1.9**  
(Previous revision: 14 December, v1.8)

*Applicability:* All VPN connections to State of Idaho's WAN  
*Policy Owner(s):* Department of Administration  
*Policy Auditor(s):* Department of Administration

# Virtual Private Network

---

## 1. Introduction

A virtual private network (VPN) is a private data network connection that makes use of the public telecommunications infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Using a virtual private network involves maintaining privacy through the use of authorization, authentication, and encryption controls that encrypt data before sending it through the public network and decrypting it at the receiving end. In a site-to-site configuration, a VPN can be contrasted with a system of owned or leased lines that can only be used by one company. In a remote user configuration, a VPN can be contrasted to a privately managed remote access system (e.g. dial-up). The concept of the VPN is to give the agency the same capabilities at much lower costs by using the shared public infrastructure rather than a private one. However, VPN links are considered to be less trusted than dedicated, private connections; therefore, this policy sets forth the security requirements for VPN connections to the State's network.

DITCS, has adopted security-industry *best practices* for VPN access that protects the State's internal network from becoming compromised through external VPN connectivity, while still allowing an agency and their users access to internal resources through the public telecommunications infrastructure.

All agencies implementing VPNs connected to the State's Wide Area Network (WAN) must adhere to this policy. This policy adheres to current standards, policies, and guidelines implemented by the ITRMC and may be subject to change as new standards, policies and guidelines are adopted.

## 2. Remote-Access Client VPN Requirements

- 2.1. Remote-access VPN users must use only ITRMC-approved VPN client software. If an Agency elects to use a VPN client software product not currently approved by the ITRMC, an exemption for such use must be approved by the ITRMC prior to use. DOA will only permit VPN client connections for ITRMC approved products (to include exemptions).
- 2.2. When establishing a VPN connection to the State's network, the VPN client software must force all traffic to and from the remote computer over the VPN tunnel; all other traffic must be dropped. The remote client must not be allowed to establish network/Internet access through a separate network/Internet connection when actively connected to the VPN (often referred to as split tunneling).
- 2.3. Remote client VPN access must be limited to only the destination agency host system(s) for which the end user has a requirement to access. All other access must be restricted.
- 2.4. Remote client VPN software must be configured to use an integrated, centrally-managed personal firewall. Additionally, the VPN client must conduct a Secure Configuration Verification check of the remote system prior to establishing a VPN tunnel to the State's network. At a minimum, these components must be configured to conduct the following security functions:
  - 2.4.1. Integrated, centrally-managed personal firewall: As part of the VPN connection, the remote client's firewall must be configured with appropriate access controls to restrict the remote user to

only required resources and network services (e.g. ports, protocols). Access controls must be based on the source, destination and type of network traffic required to be received by or sent from the client system.

2.4.2. Secure Configuration Verification (SCV) check: The remote VPN client must pass an automated Secure Configuration Verification check prior to establishing a VPN connection to the network. If the VPN client identifies that the system does not conform to the requirements of the SCV check, VPN connectivity to the State network must be denied (with the optional exception annotated in paragraph 2.4.2.1.1). This SCV check must include the following, at a minimum:

2.4.2.1. Verify the remote client OS has the most recent service pack installed (within 90 days of release of the latest service pack).

2.4.2.1.1. An agency that manages its own VPN infrastructure may elect to not immediately deny VPN access for users who do not comply with paragraph 2.4.2.1. If the agency opts to not immediately deny access, they must log non-compliant connections and notify the end-user of the requirement to update to the most recent service pack. (Note: If a known exploit is identified for a critical vulnerability (as determined by the Carnegie Mellon CERT), the end-user must apply the applicable service pack and/or security hot-fix to mitigate the risk of exploitation.)

2.4.2.2. Verify the remote client is using current anti-virus software. Virus signature files must be kept updated to the most current signatures within 10 calendar days, as supplied by the appropriate virus software vendor.

2.4.3. All new VPN client connections must be deployed with VPN software that meets these requirements. Existing remote VPN users must upgrade to new VPN client software that can fulfill these requirements no later than July 31, 2005.

2.4.3.1. Until a system is equipped with VPN software that automatically validates the SCV checks, the system must meet the SCV requirements (as stated in section 2.4.2) prior to establishing a VPN tunnel to the State's network. Agencies must annually assess that all such systems meet this requirement.

2.5. Remote-access VPN users must utilize two-factor authentication for access to the State's network. This two-factor authentication must include a hardware-based token. The remote user may use either the Enterprise authentication solution(s) or an Agency-provided authentication solution, as described below:

2.5.1. Enterprise two-factor authentication solutions: DOA will maintain an enterprise capability for VPN authentication services. VPN connections that terminate at a DOA-managed firewall/VPN device must use these authentication services. Currently, the DOA supports two forms of authentication services:

2.5.1.1. CryptoCard One-Time Password (OTP) Tokens: Users who require a high level of security are recommended to use the CryptoCard RB-1 Token. This token is the most secure two-factor authentication service offered by DOA. The CryptoCard token uses a random challenge-response scheme, ensuring the authentication process is not vulnerable to electronic eavesdropping, sniffing, or password guessing.

2.5.1.2. Rainbow iKey USB Token with Digital Certificate: The Rainbow iKey USB token is designed for users who do not require the security associated with an OTP token. The iKey token is programmed with a digital certificate from the Enterprise Certificate Authority (CA) and is protected by a passphrase (or PIN). The user must insert the USB token into the remote

computer system and then enter a passphrase. The VPN client software is then able to access the digital certificate and use this certificate to authenticate to the Enterprise VPN device.

- 2.5.2. Agency-provided authentication solutions: Agencies are encouraged to use the Enterprise solutions to minimize costs and maintain a common security architecture; however, if an Agency opts to exercise the VPN pass-through tunnel option (see Section 4), an Agency may provide its own authentication solution for VPN users, if needed. This solution must adhere to the principle of two-factor authentication, with the use of a hardware-based token.
- 2.6. The Agency must annually validate each VPN user account and determine if the account is still required. Accounts no longer required must be removed from the applicable authentication solution.
- 2.7. Remote-access VPN users must not record their passphrase or PIN on the hardware authentication token.
- 2.8. Remote-access VPN users must ensure unauthorized users are not permitted access to the State's internal network via the VPN.
- 2.9. Remote-access VPN users must be reauthenticated and/or disconnected from the network after four hours of continuous connectivity.
- 2.10. Remote VPN user identification must be attributable to a single person. User identification should be based upon an individual user's name. Group and/or office identifications are not permitted.
- 2.11. By using VPN technology with privately-owned computing equipment, users must understand that their machines become an extension of the State's internal network, and as such are subject to the same policies that apply to State-owned systems.
- 2.12. In all cases, the Agency (or its VPN user) is responsible for the purchase (initial and on-going maintenance costs, if any) of the VPN client software. For all authentication solutions, the Agency (or its VPN user) is responsible for the purchase of hardware tokens.

### **3. Site-to-Site VPN Requirements**

- 3.1. Site-to-site VPNs must use only ITRMC-approved VPN hardware and/or software, as applicable. If an Agency elects to use a VPN product not currently approved by the ITRMC, an exemption for such use must be approved by the ITRMC prior to use. DOA will only permit VPN site-to-site connections for ITRMC approved products (to include exemptions).
- 3.2. Site-to-site VPN devices must use digital certificates for device authentication to ensure the accurate identity of peer VPN devices. Digital certificates assure strong authentication and provide more scalability than pre-shared secrets.
- 3.3. Site-to-Site VPN Requirements for Remote Agency Offices:
  - 3.3.1. An Agency may elect to establish a VPN to a remote office in order to eliminate costly long-haul connections (e.g. frame-relay) with lower cost, Internet-accessible broadband connections (e.g. DSL, cable, etc). The following requirements apply specifically to such site-to-site VPN connections:
    - 3.3.1.1. There will be no unauthorized backdoor connection(s) at the remote office locations (e.g. modems, connection to other networks, etc). No other connections to the remote network will be implemented without prior notification to and authorization from DOA.

- 3.3.1.2. The remote office must deploy a firewall to protect the office from Internet-based threats. At a minimum, this firewall must be configured in accordance with DOA guidelines and/or policies.
  - 3.3.1.3. Computer systems in the remote office must employ current virus protection. Virus signature files must remain updated to the most current version supplied by the applicable virus software vendor.
  - 3.3.1.4. Computer systems in the remote office must be patched with critical security related patches within 4 weeks of when they are made available. (A critical security patch is defined as either a patch recommended by the Carnegie Mellon CERT or categorized as a "Critical" severity rating by Microsoft Corporation.)
  - 3.3.1.5. The Agency is responsible for providing and funding for its own WAN connectivity (e.g. DSL, cable, etc) and for the purchase of the VPN hardware, software and related maintenance.
- 3.4. Site-to-Site VPN Requirements for Contractors/Business Partners:
- 3.4.1. An Agency may elect to establish a VPN to a contractor and/or business partner to improve communications capabilities and minimize costs.
  - 3.4.2. Site-to-site VPNs may be established with a third-party (such as a contractor and/or business partner). This type of VPN may terminate at the State's Enterprise VPN devices or at an Agency-level VPN device (assuming the Agency is in compliance with Section 4, *VPN Pass-Through Tunnels*.)
    - 3.4.2.1. The security architecture and configuration of such connections must be reviewed on an annual basis, since the remote device is not typically under the administrative control of the State.
  - 3.4.3. Traffic permitted through the VPN tunnel from the remote Contractor/Business Partner's network must be restricted to only specific Enterprise and/or Agency resources (based upon the business requirements for that connection). All other traffic must be dropped.
    - 3.4.3.1. Business partner traffic should not mix with the Agency's intranet traffic. Business partner traffic should be restricted by a firewall to a protected segment of the Enterprise and/or Agency's network.

## 4. VPN Pass-Through Tunnels

- 4.1. Agencies are encouraged to use the Enterprise VPN capabilities to ensure a common security posture and minimize overall State costs for VPN management. However, in order to meet specific Agency business needs, an Agency may request to have a VPN pass-through tunnel. This tunnel will allow the VPN connection to traverse the Enterprise security perimeter and terminate at an Agency-level VPN device.
  - 4.1.1. The DOA will permit such VPN pass-through tunnels; however, such tunnels are restricted to one IP address per agency. This restriction minimizes the vulnerability surface for the State's enterprise network, while also addressing manageability and scalability issues on the Enterprise perimeter firewalls. (Note: A VPN pass-through tunnel may be configured to terminate at two IP addresses per agency, only when supporting a redundant architecture.)

4.1.2. Only the following ports and/or protocols will be permitted through the Enterprise security perimeter to support an Agency VPN pass-through tunnel using either IPSEC or SSL:

4.1.2.1. Using IPSEC:

- 4.1.2.1.1. Internet Key Exchange Protocol (TCP & UDP Port 500)
- 4.1.2.1.2. IPSec Encapsulating Security Payload (IP Protocol 50)
- 4.1.2.1.3. IPSec Authentication Header Protocol (IP Protocol 51)
- 4.1.2.1.4. IPSec NAT Traversal (UDP Port 4500)

4.1.2.2. Using SSL:

- 4.1.2.2.1. SSL (TCP 443)

4.2. Agencies who elect to use the VPN pass-through option must adhere to all requirements identified within this policy and submit a signed copy of the *Request for VPN Pass-Through Tunnel* (Appendix A) to the Department of Administration's Division of Information Technology and Communication Services.

4.3. DOA will conduct periodic reviews of an Agency's VPN implementation. At a minimum, reviews will be conducted annually; however, reviews may be conducted more frequently as needed. The purpose of these audits are to ensure VPN pass-through tunnels are secure and adhere to existing policies. These assessments will provide a direct benefit to the agency while also ensuring the VPN cannot be used maliciously to gain access into other parts of the State's network.

4.3.1. DOA will provide the agency a report of audit findings upon conclusion of the audit.

4.3.2. If an Agency VPN implementation is in violation of existing security policies, DOA will work with the Agency to resolve any outstanding issues. However, if the Agency and/or DOA are unable to address the security concerns in a timely manner, the applicable VPN access to the State's network may be disabled until the VPN implementation adheres to applicable policies.

## 5. VPN Technical Requirements (IPSec & SSL VPNs)

5.1. When deploying a VPN, the following technical settings/requirements must be adhered: (As new encryption/hashing algorithms are introduced, the policy will be reviewed to determine if any changes should be made.)

5.1.1. IPSEC

5.1.1.1. Key Exchange Encryption Algorithm: 3DES or AES (256-bit)

5.1.1.2. Data Integrity: SHA-1

5.1.2. SSL

5.1.2.1. 128-Bit Encryption Certificate (Verisign)

## 6. Escalation & Resolution Procedures

6.1. The technical staff within an Agency and DOA will work collaboratively and proactively to resolve issues associated with this policy; however, in the event that issues cannot be resolved amongst the staffs, the following Escalation & Resolution levels will be followed. The agency and DOA will make every attempt to resolve issues at the lowest level.

Escalation Level	DOA Point of Contact (POC)
A	IT Manager, DITCS
B	Administrator, DITCS
C	Director, DOA
D	ITRMC

6.2. If an issue needs to be escalated, the following procedures will be followed:

- 6.2.1. Escalation Level A, B, & C: The escalating agency Point of Contact (POC) will request a meeting with the DOA first level Point of Contact (POC) to discuss the issue. These POCs will attempt to resolve the issue by evaluating the security risk to the State of Idaho's network while also balancing the need to meet agency's business requirements. Upon the completion of this meeting, the POCs will jointly document the issue and their decision. If resolution cannot be found, the issue will be forwarded to the next escalation level.
- 6.2.2. Escalation Level D: In the unlikely event that an issue cannot be resolved prior to or at Escalation Level C, each agency will document their position and forward this document to the ITRMC POC for a decision by the ITRMC or its designated representative/committee.

## Appendix A

### Request for VPN Pass-Through Tunnel

In order to meet the \_\_\_\_\_'s business needs, we hereby request  
*(insert Department/Agency name)*

the appropriate configuration changes to enable a VPN pass-through tunnel to our environment.

I have read, understood, and agree to the VPN Connectivity and Management Policy.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Agency IT Director/Manager  
*(Signature)*

\_\_\_\_\_  
Agency IT Director/Manager  
*(Printed name)*

**Appendix B**

**Request for VPN Remote Client Access for a Contractor to DoA owned Equipment**

In order to meet the \_\_\_\_\_'s business needs, we hereby request  
*(insert Department/Agency name)*

the appropriate configurations be implemented to enable our contractor \_\_\_\_\_ to  
*(insert provider's name)*  
gain VPN access into the state's environment.

The contractor agrees that their client equipment contains a centrally-managed personal firewall, the client OS has the most recent service pack installed, and the client is using current anti-virus software. Virus signature files are kept updated to the most current signatures available. The contractor must notify DoA System Administrator's at a minimum 4 hours in advance of when they will be making modifications to the agency's applications or data housed on DoA owned servers. Contractor agrees to limit their access to the applications and/or data directly related to the agency's project and will not make any system or services modifications of any kind to the DoA servers.

The provider must list below all employees that will be issued VPN access to the state's network. Remote VPN user identification must be attributable to a single person. User identification must be based upon an individual user's name. Group and/or office identifications are not permitted.

_____	_____
_____	_____
_____	_____

We have read, understood, and agree to the VPN Connectivity and Management Policy.

Date: \_\_\_\_\_

Date: \_\_\_\_\_

\_\_\_\_\_  
*Agency IT Director/Manager signature*

\_\_\_\_\_  
*Provider's signature*

\_\_\_\_\_  
*Agency IT Director/Manager printed name*

\_\_\_\_\_  
*Provider's printed name*