



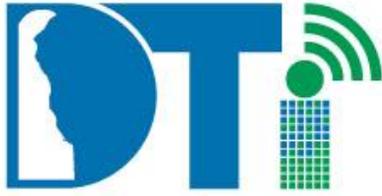
STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
 801 Silver Lake Blvd.
 Dover, Delaware 19904

Doc Ref Number:	DTI-0058.01	Revision Number:	5
Document Type:	Enterprise Policy	Page:	1 of 7
Policy Title:	VPN Policy		

Synopsis:	To standardize a security policy and guideline for the State of Delaware agencies, public schools, Offices of Elected Officials, Courts and Legislature connecting to internal data communications networks from remote locations or from networks other than their primary user network.		
Authority:	Title 29, Delaware Code, §9004C - General powers, duties and functions of DTI "2) Implement statewide and interagency technology solutions, policies, standards and guidelines as recommended by the Technology Investment Council on an ongoing basis and the CIO, including, but not limited to, statewide technology and information architectures, statewide information technology plans, development life cycle methodologies, transport facilities, communications protocols, data and information sharing considerations, the technique of obtaining grants involving the State's informational resources and the overall coordination of information technology efforts undertaken by and between the various State agencies;"		
Applicability:	This Policy is applicable to all users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.		
Effective Date:	August 14, 2006	Expiration Date:	None
POC for Changes:	Elayne Starkey, Chief Security Officer		
Approval By:	James Collins, State Chief Information Officer		
Approved On:	August 14, 2006		



"Delivering Technology that Innovates"



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	DTI-0058.01	Revision Number:	5
Document Type:	Enterprise Policy	Page:	2 of 7
Policy Title:	VPN Policy		

TABLE OF CONTENTS

Section	Page
I. Policy	2
II. Definitions	6
III. Development and Revision History	6
IV. Approval Signature Block	6
V. Listing of Appendices	7

I. Policy

Any and all projects, consulting requests, support, maintenance or development requirements and current authorizations will be subject to review for compliance with this policy.

Summary:

This policy establishes SSL-VPN as the VPN technology adhered to in compliance with the State of Delaware security policy and best practice to protect internal networks, devices, and hosts from external security threats posed by transmitting data over the Internet, other external networks, or other departmental networks within the State.

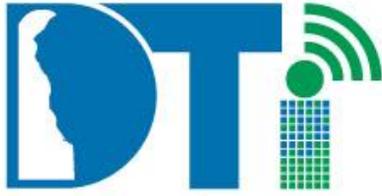
VPN provides personal computer or workstation authentication, integrity and confidentiality through encryption and anti-replay security services. Authentication will be achieved using only enterprise approved methods.

Objectives:

- To protect the State of Delaware systems from unauthorized use.
- To increase the level of security inherent in the State of Delaware network infrastructure.
- To comply with State and Federal data protection guidelines.



“Delivering Technology that Innovates”



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	DTI-0058.01	Revision Number:	5
Document Type:	Enterprise Policy	Page:	3 of 7
Policy Title:	VPN Policy		

- To prevent alteration, destruction, or modification of host or system information.
- To prevent disclosure of protected information to unauthorized individuals.
- To decrease the risk of disruption or interruption of network service levels.

Benefits Expected:

- Accommodate appropriate and reasonable access to state resources.
- Increased security for internal hosts and networks.
- Increased enforcement of enterprise level security policies.
- Maintain acceptable levels of network management efficiency.
- Increased ability to audit.

Applicability:

This policy applies to browser connections from desktops, laptops or workstations that require access to any internal State of Delaware system, server or network connected host.

This policy applies to cross-network access. **Cross-network access** is defined as any State of Delaware employee, contractor or partner connection crossing any State of Delaware trusted network perimeter. An example of this type of access would be connecting to an internal destination host from the public Internet, across the education network or across a designated VRF. A VRF (virtual routing/forwarding instance) is used to segment departmental networks and will define the VPN inheritance of each user and site.

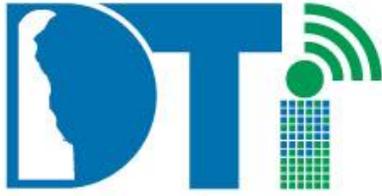
Assumptions:

Remote users shall access the State of Delaware network(s) and networked resources only with approved equipment, configured with current software and anti-virus.

It is assumed that agency or host administrators provide appropriate security through best practices applicable to application level, network and host security.

The Information Security Officer (ISO) must thoroughly review and understand all requests and applicable standards and policies prior to approval.





STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	DTI-0058.01	Revision Number:	5
Document Type:	Enterprise Policy	Page:	4 of 7
Policy Title:	VPN Policy		

Implementation Considerations:

Customers must coordinate their remote access needs with the DTI Telecommunications Team and review the security risk threat profile with the security team. Any access outside of the United States must be approved by DTI.

The standard State of Delaware VPN configuration does not necessarily meet specific federal or industry compliance requirements. Agencies must adhere to applicable rules and regulations of the appropriate governing bodies in regards to access of information via VPN. For example Federal Tax Information (FTI) access via VPN must comply with [IRS 1075 Rev 10-2014](#). Agencies must request custom configurations from DTI if access beyond the standard VPN offering is required.

The ISO is responsible for ensuring that all remote access to the State’s network(s) is terminated immediately when there is a separation of service. All remote access should be reviewed when there is a change in position, or any change in requirements for remote access. The ISO must ensure that the least amount of access required is provided.

Remote users shall only use access for approved purposes.

At no time should any employee, vendor or account holder provide their login or user information or password to anyone.

DTI will on occasion schedule outages of VPN services for the purposes of required maintenance.

Note: *Other methods of performing the required functions will be explored prior to considering remote access. Assignment of VPN privileges will be at the discretion of the DTI security staff and will be based on the evaluation of threat versus requirement. Revocation of VPN privileges will be at the discretion of the DTI security staff if a user is suspected of policy violation.*

Access Availability:



“Delivering Technology that Innovates”



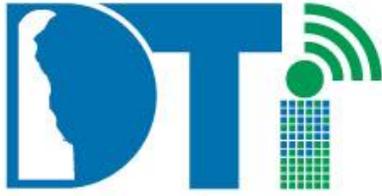
STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	DTI-0058.01	Revision Number:	5
Document Type:	Enterprise Policy	Page:	5 of 7
Policy Title:	VPN Policy		

- All state employees will be provided access to e-mail and calendaring via the (OWA) Outlook Web Access site.
- State employees needing access to file shares and systems will require an SSL-VPN account. Access will be provided to file shares and systems within the customer's VRF.
- Systems Administrators and/or approved Telecommuters requiring access will be provided with management protocols consistent with the standard (e.g. RDP, SSH) to devices within their customer's internal network (VRF) or within a DMZ. Multi-factor authentication is a requirement of this access.
- Vendors or Contractors** will be provided with management protocols consistent with the standard to systems within the DMZ.
- Authentication requirement may be modified based on requested access.

**Vendors and/or Contractors will receive *named accounts* only that expire on the anniversary date of issuance; they must have a current contract, pass a criminal background check and sign the appropriate confidentially and non-disclosure forms. For more information on the criminal background check requirement, see the Security Clearances section of the [Delaware Information Security Policy](#).





STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	DTI-0058.01	Revision Number:	5
Document Type:	Enterprise Policy	Page:	6 of 7
Policy Title:	VPN Policy		

II. Definitions

None.

III. Development and Revision History

Initial version established December 16, 2004.
Reformatted August 14, 2006.
Revised September 17, 2007.
Revised December 18, 2008.
Revised December 16, 2009. Update CIO.
Revised November 5, 2010.
Revised March 15, 2012.
Revised February 6, 2013.
Revised October 15, 2013. Update POC.
Revised April, 21 2016. Add FTI language.

IV. Approval Signature Block

On File	
Name & Title: James Collins State Chief Information Officer	Date April 21, 2016



"Delivering Technology that Innovates"



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	DTI-0058.01	Revision Number:	5
Document Type:	Enterprise Policy	Page:	7 of 7
Policy Title:	VPN Policy		

V. Listing of Appendices



"Delivering Technology that Innovates"