I. Authority, Applicability and Purpose

A. Authority: Title 29, Chapter 90C of the Delaware Code provides broad statutory authority to the Department of Technology and Information to implement statewide and interagency technology solutions, policy, standards and guidelines for the State of Delaware’s technology infrastructure. “Technology” means computing and telecommunications systems, their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information or data electronically. The term “technology” includes systems and equipment associated with e-government and Internet initiatives.

B. Applicability: Applies to all 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 funding, access, and continued use of these resources.

C. Purpose: This standard will address technology used to access the State’s information assets from remote locations. The need exists to provide safe and private access to the State’s resources. This standard will establish the acceptable methods of remote access.

II. Scope

A. Audience: This document is intended for Systems Administrators, Network Administrators, and end user support personnel. This document is not intended for use by non-IT personnel.
These standards are adopted by the Department of Technology and Information (DTI), through the Technology and Architecture Standards Committee (TASC), and are applicable to all Information Technology use throughout the State of Delaware. Any questions or comments should be directed to dti_tasc@state.de.us.
2. **Remote Access Server**—The computer and associated software that is set up to handle users seeking access to the network remotely. Sometimes called a *communication server*, a remote access server usually includes or is associated with a **Firewall** server to ensure security and a **router** that can forward the remote access request to another part of the corporate network. A remote access server may include or work with a modem pool manager so that a small group of modems can be shared among a large number of intermittently present remote access users. A remote access server may also be used as part of a virtual private network (**VPN**)\(^1\).

3. **Terminal Services**—Allows remote computers to run applications on a server as though it is running locally. This is similar to the functionality provided by X on UNIX and Linux platforms. Keystrokes and mouse action information is sent from the client to the server over the network and visual display information is sent back to the client from the server.

4. **Remote Desktop**—Taking control of a target computer. This means, for example, that you can connect to your work computer from home and have access to all of your applications, files, and network resources as though you were in front of your computer at work.

5. **Remote Administration**—Performing Network or Systems Administrator tasks on a computer other than the one at which you are sitting.


### B. Declarations

1. When access is through a public terminal (library PC, Kiosk, etc.) password managers, or forms completion programs must not be utilized to remember either logon ID or password.

2. All Remote Access requires SSL-VPN in compliance with **VPN Policy**.

3. Remote vendor support is required to be initiated and monitored by the initiating employee.

4. Non-State entities are not permitted unattended remote access to State of Delaware network or computing resources.

\(^1\) [http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212887,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212887,00.html)
V. Definition of Ratings

Individual components within a Standard will be rated in one of the following categories:

<table>
<thead>
<tr>
<th>COMPONENT RATING</th>
<th>USAGE NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and solidly positioned in its product life cycle.</td>
<td>These components can be used without explicit DTI approval for both new projects and enhancement of existing systems.</td>
</tr>
<tr>
<td>DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete.</td>
<td>Via the State’s waiver process, these components must be explicitly approved by DTI for all projects. They must not be used for minor enhancement and system maintenance without explicit DTI approval via the State’s waiver process.</td>
</tr>
<tr>
<td>DISCLAIMED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.</td>
<td>No waiver requests for new solutions with this component rating will be considered.</td>
</tr>
</tbody>
</table>

**Missing Components** – No conclusions should be inferred if a specific remote access technology is not listed. Instead, contact TASC to obtain further information.
VI. Component Assessments

A. N/A