Standard ID:	**SE-VP-001**
Title:	**Virus Protection**
Domain:	**Security**
Discipline:	**Network Security**
Effective Date: Revision no.: Original date:	**02/16/2018** **5** **1/01/2005**

I. Authority, Applicability and Purpose

A. **Authority:** Title 29, Chapter 90C 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:** Due to the insecurity of the Internet, a need exists to secure the State's digital assets such as data and computers. This standard covers protecting those digital assets from computer viruses, spyware, worms, and trojans, etc.

II. Scope

A. **Areas Covered:** This standard covers all State digital assets.

B. **Environments:** This standard applies to all Desktops, Laptops, Servers and personal computers belonging to the State. This standard also applies to computers belonging to employees of the State of Delaware and those external businesses and Governments whose computers interact with the State's digital assets behind our firewall. This standard covers all servers including, but not limited to file, mail, messaging, data base, web, application, print, middleware, voice, load balancer, failover, test, production, and development owned and operated by the State. It covers all State servers under contract by 3rd parties. This standard does not cover appliances like firewalls, or routers.

III. Process

A. **Adoption:** – These standards have been 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.

B. **Revision:** – Technology is constantly evolving; therefore the standards will need to be regularly reviewed. It is the intent of the TASC to review each standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. **Contractors:** – Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@state.de.us.

D. **Implementation responsibility:** DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. **Enforcement:** DTI will enforce these best practices during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These best practices may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. **Contact us:** – Any questions or comments should be directed to dti_tasc@state.de.us.

IV. Definitions/Declarations

A. Definitions

1. **Secure** – Means ensuring that only the intended recipient can read the message, and also guaranteeing that it was not intercepted, or modified, and that it was delivered. This requires that email be protected, controlled, tracked and recallable
2. **Spyware** – http://en.wikipedia.org/wiki/Spyware
3. **Trojan** – http://en.wikipedia.org/wiki/Trojan_horse_(computing)
4. **Virus –** http://en.wikipedia.org/wiki/Computer_virus

5. **Worm –** http://en.wikipedia.org/wiki/Computer_worm

B. Declarations

1. Updates must be provided automatically on a consistent, recurrent schedule.
2. Must be compatible with the State's digital infrastructure.
3. Must be covered under an Enterprise-wide license.
4. Steps must be taken to ensure that removable media such as ZIP disks, USB sticks, USB hard drives, USB memory, etc. when used, must be connected to a device that is virus protected.

V. Definition of Ratings

Individual components within a Standard will be rated in one of the following categories. **COMPONENT RATING**	**USAGE NOTES**
• **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.	These components can be used without explicit DTI approval for both **new projects** and **enhancement** of existing systems.
• **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.	These components must be explicitly approved by DTI for **new projects**. They can be used for **minor enhancement** and **system maintenance** without explicit DTI approval.
• **DISALLOWED** – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.	

A. Missing Components – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC dti_tasc@state.de.us to obtain further information.

VI. Component Assessments

A. Scope: The State provides an Enterprise-Wide Virus Protection solution for use in all PCs and servers. This solution is managed centrally by DTI. Instructions for its use can be found on the DTI Internet page.

B. Centralized reporting: It is vitally important for DTI to be aware of Virus activity within the State Network. It is very seldom that virus outbreaks stay local and it is imperative that DTI receive timely notifications in order to take action to protect the rest of the State Network. DTI purchases and distributes McAfee to all agencies for use on gateways, servers, workstations and provides for individual state employee use at home. DTI Utilizes McAfee's EPO to handle distribution and centralized reporting. Agencies opting not to use the provided State service must at least provide some means of sharing real-time reporting with DTI's core monitoring infrastructure.

#	Component	Rating	Comments
1	Crowdstrike Falcon	Standard	3-year migration beginning 2017 will make this the Enterprise solution.
2	McAfee VirusScan	Declining	Transitioning to Crowdstrike Falcon.
3	Symantec	Standard	Currently utilized by K-12.
4	Other Virus Protection Packages for Desktops that participate in DTI's centralized virus protection reporting (McAfee's EPO).	Declining	For non-State employees, or businesses and non-State of Delaware government agencies doing business with the State's digital assets. Or for an Agency that is not currently utilizing one of the solutions mentioned above: Any up-to-date, automatically updated commercial Virus Protection package that provides some means of sharing real-time reporting with DTI's core monitoring infrastructure. (McAfee's EPO).
5	Other Virus Protection Packages for Desktops not capable of participating in DTI's centralized virus protection reporting. (McAfee's EPO)	Disallowed	Agencies opting not to use the provided State service must at least provide some means of sharing real-time reporting with DTI's core monitoring infrastructure.
6	McAfee NetShield	Disallowed	