Standard ID:	**PL-SEOS-001**
Title:	**Platform Operating Systems Software**
Domain:	**Platform**
Discipline:	**Software**
Revision Date: Revision no.: Original date:	**12/10/2020** **9** **09/01/2004**

I. Authority, Applicability and Purpose

A. Authority: Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO.

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 the operating systems of the server segment of the State of Delaware's computer infrastructure. The need exists to reduce security vulnerabilities and system administration effort in a cost effective manner in this huge and ever-growing investment. The modern data center is being inundated with new and ever-expanding needs for servers. The driving forces behind this need are:

- The increasing workload of modern business to meet privacy and confidentiality regulations,
- The need to segment tiers of operating environments into Presentation, Application and Data Base for security, privacy and operational efficiencies,
- The complexity of and the myriad solutions needed to satisfy today's business needs for faster and more comprehensive response to citizen's needs,
- Security threats from the Internet and elsewhere.

II. Scope

A. Audience: This document is intended for Systems Administrators, Network Administrators, Computer Auditors, and server support personnel. This document in not intended for use by non IT personnel.

B. Functions: This standard will cover all servers owned and operated by the State. It will cover all State servers under contract by third parties. This standard does not cover appliances like firewalls, or routers. This standard does not cover appliances that have embedded operating systems.

C. Areas Covered: Only operating systems are covered by this standard, not applications, or utilities (Virus protection, pop-up blockers, etc).

D. Platforms: Only servers are covered by this standard

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) group.

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. **Appliance** – A computer architected for a specific task. The operating system is designed for a specific function rather than for general application.
2. **Application:** For the purpose of this standard, an application is defined as a multi user application and/or back end process that supports Moderate or higher critical business processing as defined in the DR/BCP classifications found in the Delaware Information Security Policy.

3. **Firewalls** – A device (logical or physical) that is used to block unauthorized communications to network devices (i.e. servers) while also permitting authorized communications.
4. **Linux –** A Unix-like computer operating system. The name "Linux" comes from the Linux kernel started in 1991 by Linus Torvalds. Linux is one of the most prominent examples of free software and open source development: typically all underlying source code can be freely modified, used, and redistributed by anyone. The system's utilities and libraries usually come from the GNU operating system, announced in 1983 by Richard Stallman. The GNU contribution is the basis for the alternative name GNU/Linux. Linux appears in many commercial operating systems like Red Hat and Novell's SUSE, and also in many non-commercial varieties, like Debian, Gentoo, Knoppix and others. In all, there are hundreds of "distributions", or Linux based operating systems, available for download on the internet, free of charge.
5. **Operating System:** Software that coordinates various activities of the computer (e.g. memory management, and shared libraries) and mediates between application software and computer hardware (e.g. print services).
6. **Server**: A hardware device on a network that manages resources such as printers, files and applications. The intent of this hardware device is to provide benefit to more than one person at a time.
7. **UNIX –** A computer operating system originally developed in 1969 by a group of AT&T employees at Bell Labs including Ken Thompson, Dennis Ritchie and Douglas McIlroy. Today, the definition of UNIX ® takes the form of the worldwide Single UNIX Specification integrating X/Open Company's XPG4, IEEE's POSIX Standards and ISO C. Through continual evolution, the Single UNIX Specification is the defacto and du jour standard definition for the UNIX system application programming interfaces. There is also a mark, or brand, that is used to identify those products that have been certified as conforming to the Single UNIX Specification, initially UNIX 93, followed subsequently by UNIX 95, UNIX 98 and now UNIX 03. The Open Group holds the definition of what a UNIX system is and its associated trademark in trust for the industry.

B. Declarations

1. All server operating system must be in compliance with the State's Software Policy.

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.	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.
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 operating system is not listed. Instead, contact the TASC to obtain further information.

VI. Component Assessments

Component	Rating	Comments
IBM zSeries		
z/OS	Standard	Version 2.1.x and above
LINUX		
Oracle Enterprise Linux	Standard	Note 1: When an OS's EOL date is greater than 3 years of the go-live date of the new implementation. Must be supported for security patching.
Oracle Enterprise Linux	Declining	Note 2: When the OS's EOL date is less than 3 years, no new implementations of the OS are permitted. Must be supported for security patching.
Oracle Enterprise Linux that is End of Life (EOL)	Disallowed	Note 3: EOL OS's. Existing OS's must be turned off by the OS's EOL date.
Red Hat Enterprise Server Linux **ES**	Standard	Note 1: When an OS's EOL date is greater than 3 years of the go-live date of the new implementation. Must be supported for security patching.
Red Hat Enterprise Server Linux **ES**, **AS**	Declining	Note 2: When the OS's EOL date is less than 3 years, no new implementations of the OS are permitted. Must be supported for security patching.
Red Hat Enterprise Server Linux **ES, AS, WS** that is End of Life (EOL)	Disallowed	Note 3: EOL OS's. Existing OS's must be turned off by the OS's EOL date.
CentOS Linux	Standard	Note 1: When an OS's EOL date is greater than 3 years of the go-live date of the new implementation. Must be supported for security patching.
CentOS Linux	Declining	Note 2: When the OS's EOL date is less than 3 years, no new implementations of the OS are permitted. Must be supported for security patching.

CentOS Linux	Disallowed	Note 3: EOL OS's. Existing OS's must be turned off by the OS's EOL date.
Any unspecified Linux Distribution	Standard	Customer must make arrangements for support
Any unspecified Linux Distribution that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.
MAC OS		
MAC OS X	Standard	Version 10.10 and above, customer must make arrangements for support
MAC OS X that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.
UNIX		
HP-UX	Standard	Version 11i v3 and above
HP-UX	Declining	Version 11i v1 and v2
HP-UX that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.
Unix System Services	Standard	Included with z/OS
Oracle Solaris	Standard	Version 10 and above, customer must make arrangements for support
Oracle Solaris that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.
IBM AIX	Standard	Customer must make arrangements for support
IBM AIX that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.
SGI IRIX	Disallowed	Support ended in 2013.
SGI IRIX that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.
Any unspecified Berkley Software Distribution (BSD)	Standard	Customer must make arrangements for support

Any unspecified Berkley Software Distribution (BSD) that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.
Virtualization Host O/S		
HP-UX 11i Virtual Partitions	Standard	Version A.03.XX and above
IBM z/VM	Standard	Version 6.3 and above
VMware vSphere	Standard	Version 6 and above
VMware vSphere	Declining	Version 5 and below
VMware ESX	Declining	Version 3.5 and above
Windows OS		
Windows Server	Standard	When an OS's EOL date is greater than 3 years of the go-live date of the new implementation, it is acceptable. Existing OS's must be life cycled or turned off by the OS's EOL date.
Windows Server	Declining	When the OS's EOL date is less than 3 years, no new implementations of the OS. Existing OS's must be life cycled or turned off by the OS's EOL date.
Windows Server that is End of Life (EOL)	Disallowed	Existing OS's must be turned off by the OS's EOL date.