Standard ID:	AR-SYSARCH-001
Title:	**Systems Architecture**
Revision Number:	10
Domain:	Architecture
Discipline:	Systems Design Architecture
Effective:	7/1/2023 (new systems), 3/1/2024 (existing systems)
Reviewed:	12/15/2022
Approved By:	Chief Operating Officer, Chief Security Officer
Sponsor:	Chief Operating Officer, Chief Security Officer

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. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as Local Education Agencies, 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 communicates how to construct IT solutions intended for production status. A good architecture builds into itself the ability to change not only in expected ways, but also in unexpected ways. This standard addresses systems from a high level and from the viewpoint of data and who is accessing a system. This standard will continue to evolve and enhance the understanding of Systems Architecture within the State.
.

II. Scope

A. **State of Delaware:** Project Leaders, Application Developers, Systems Administrators, Network Administrators, IT Security Personnel, Computer Auditors, and their managers and application development contractors for the State are the intended audience. IT personnel are the only intended users of this document.

B. **Areas Covered:** This standard will cover all State on-premise systems and systems that utilize IaaS.

C. **Environments:** All technology environments are covered except Mainframe systems.

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 this 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@delaware.gov.

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@delaware.gov.

IV. Definitions/Declarations/Controls

A. Definitions

1. Control - an effective technique to guide the design of a system that satisfies the organization's requirements.
2. Pattern – a collection of controls applied in a reference architecture, enabling consistent design and deployment of systems.
3. System components – an operating system, hardware, software, etc.
4. Advanced Web Application Firewall – this is a solution that is focused on protecting web applications and APIs. The protection methods are consistent with industry practices, are application and protocol aware, and include behavior-driven protection mechanisms.
5. North-South and East-West network traffic – North-South refers to ingress/egress traffic to a subnet. East-West refers to lateral network traffic within a subnet.
6. Network level filtering – filtering of traffic implemented at the network subnet boundary.
7. Demilitarized zone (DMZ) – a physical or logical subnet whose resources are separated from other networks. Examples
   - Internet-facing app DMZ – designed for internet/external facing solutions where only applications reside.
   - management DMZ – designed for internal solutions where IT management solutions reside.
   - 'xxx' DMZ – a specific design to match the requirements.

B. Declarations

1. Patterns will be established to document a specific use case that satisfies the system controls.
2. Mandatory State enterprise services must be used in systems as defined in the Enterprise Services Standard.
3. Services must be configured to listen on well-known ports or reasonable alternative (associated with correct protocol). Utilize IANA.
4. Use the State's Enterprise Service 'Identity & Access Management' to authenticate employee, vendor, and constituent identities when accessing State applications and systems.
5. Authenticate access to non-public applications or data
6. All Internet access to the web application or API (xml, REST, etc) must be front-ended by the State's Enterprise Service 'Advanced Web Application Firewall' which is web protocol and web application aware.

- Provide any synchronous application integration via API call or via asynchronous methods such as flat file transfer.
- If not using API or flat file transfer for integration with a third party (vendor, SaaS, PaaS, IaaS, etc), private network communication will be required (ipsec tunnel, extranet, etc) and all system architecture standards apply to the related communication.

7. Design your applications to scale according to the user audience.
8. The following insecure protocols are forbidden for user to system access: SMB, RPC, Netbios, NFS.
9. The use of an encrypted tunnel to bypass network security controls or otherwise obfuscate communication is not permitted. Scenarios or designs that utilize client VPN or IPSec tunnels to secure communication in-flight are generally acceptable.
10. Infrastructure components other than servers should use centralized admin authentication or centralized automated management of accounts (e.g. appliances, ilo's etc)
11. Each system must have an identified business sponsor and technical owner.
12. All system components must be on supported versions and updates applied on a regular scheduled basis, including vendor/3rd party supported solutions.
13. When considering design in cloud environments, use native tooling that satisfies the required controls wherever possible. For example, in AWS leverage S3 buckets for object storage and Security Groups for policing east-west traffic.
14. Due to the integrity and availability requirements of production business applications, development business applications should not communicate with production business applications.
15. Only DTI approved devices may span network segments.
16. System architecture compliance must be reviewed when the system is life cycled.
17. When possible, establish and maintain unidirectional management DMZs.
18. No conclusions should be inferred if a specific topic is not listed. Instead, contact the TASC to obtain further information.

C. Controls

- SYS1 - Limit connections to (north-south) and between the application components network socket listener(s), including lateral movement (east-west) within the same network segment.
- SYS2 - Ensure there is network isolation between business systems/applications and supporting infrastructure/management platforms.
- SYS3 - Protect data in transit. Typically, this is provided by encryption.
- SYS4 - Protect data at rest. Typically, this is provided by encryption.
- SYS5 - Utilize application/protocol aware filtering methods to detect and protect our assets such as servers, applications, data. For example, IPS, WAF, Fail2Ban, and other tools.
- SYS6 - Maintain robust north/south internet protections appropriately for the exposed service (such as brute force protections, protocol level attacks, botnet and malicious ip blocklisting).
- SYS7 - Log user authentication events to the State's Log Management and SIEM service.
- SYS8 - Use allow-listed controls for outbound internet access.
- SYS9 - Establish centralized system admin authentication or centralized automated management of accounts to servers. For example, servers Active Directory joined, or Ansible managed user accounts.
- SYS10 - Enable server logging, vulnerability scanning, and protections from risks such as malware.
- SYS11 - Management and infrastructure communication must be limited and secured to that which is needed to support the business application. For example, Solarwinds agent communication, SNMP, Splunk, etc, must be scoped to that which is required for the function of the tool.
- SYS12 - Manage and secure the integration to user and system directories such as Active Directory.
- SYS13 – Network level filtering must exist between Systems and Users.

V. Development and Revision History

Date	Revision
3/19/2007	Rev 0 – Initial version
12/15/2022	Rev 10 – Complete rewrite with a focus on controls and patterns