1.0 PURPOSE

The purpose of this policy is to provide configuration management requirements for Ohio Department of Administrative Services (DAS)-managed information systems. A strong configuration management practice will improve security by assisting in vulnerability detection and allowing for faster problem resolution; thereby, restoring services more efficiently. It will also improve overall change management procedures by decreasing the opportunity for the introduction of new incompatibilities or problems, targeting unnecessary duplication and aiding in the identification of potential license issues.

A glossary of terms found in this policy is located in Section 8.0 Definitions. The first occurrence of a defined term is in bold italics. In addition, references to National Institute of Standards in Technology (NIST) Special Publication (SP) 800-53 family identifiers and control numbers are provided in parentheticals next to requirement headers, where applicable.

2.0 SCOPE

The scope of this policy includes any DAS-managed information system.

This policy also applies to DAS data owners, service owners, and extends to managed service providers.

3.0 BACKGROUND

Unauthorized changes can adversely impact information system confidentiality, integrity and availability by introducing improperly configured systems into the network, to include poorly developed software or even malicious code. To mitigate this risk, configuration management must be applied over the life cycle of enterprise architectures, system hardware and software, and also related documentation. Effective and continuous configuration management will allow changes to information systems to be detected faster and vulnerabilities to be remediated sooner.

4.0 REFERENCES

4.1 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and
Organizations: NIST SP 800-53 provides guidelines for selecting and specifying security controls for federal government information systems.

4.2 **Ohio Administrative Policy IT-03, Software Licensing**: Ohio Administrative Policy IT-03 requires state agencies to establish controls for the use and protection of licensed software required to conduct official state business.

4.3 **Ohio Administrative Policy IT-13, Data Classification**: Ohio Administrative Policy IT-13 provides a data classification methodology to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality.

5.0 **POLICY**

Configuration management practices shall be established that include procedures for documenting DAS-managed information system configurations and guidance for how configurations are implemented, changed, and maintained. A strong configuration management practice provides a methodology designed to increase the integrity, availability, and security of DAS-managed information systems.

5.1 **Baseline Configuration (CM-2)**: All DAS-managed information systems shall have a formal, documented baseline configuration. This configuration is maintained by the applicable operations unit and serves as the baseline for all future builds. DAS-managed information system baseline configurations shall contain the following:

- System components, such as standard software packages installed for workstations, laptops, tablets, servers, mobile devices, etc.
- Current version numbers of operating systems and software applications
- Current patch information
- Configuration settings and parameters
- Network topology
- Placement of hardware within the system architecture

5.1.1 **Test and Development Baselines**: DAS-managed information system baseline configurations shall be documented and maintained for test and development environments.

5.1.2 **Baseline Exceptions**: DAS system owners shall document and maintain exceptions to DAS-managed information system baselines.

5.1.3 **Baseline Maintenance**: Baseline documentation shall be updated, as needed, based on system changes, ranging from minor configuration changes to major
system upgrades. DAS-managed information system changes shall be approved through a change control board.

5.1.3.1 Data owners and service owners shall review established baselines annually or after major DAS-managed information system changes (e.g., architectural changes that extend beyond minor patching or minor hardware maintenance, including the addition of new hardware components or software modules and/or major software upgrades; changes that enhance, interrupt or otherwise modify user experience and the way the user interacts with the system; and any change that involves system availability impacts and/or changes to operational processes).

5.1.3.2 Previous baseline configurations shall be retained in accordance with DAS record retention requirements.

5.2 Configuration Change Control (CM-3): Service owners shall establish a change control process that includes the Office of Information Security and Privacy’s (OISP) review and approval.

5.2.1 All changes to DAS-managed information systems shall be reviewed and approved through a change control process.

5.2.2 Unapproved changes to DAS-managed information systems shall be prohibited.

5.2.3 Prior to implementing a change, service owners shall notify OISP, IT management, data owners and technical teams.

5.2.4 Changes to DAS-managed information systems shall be thoroughly tested, validated and documented prior to implementation.

5.2.4.1 The documentation shall include evidence of testing, with successful completion.

5.3 Change Control Board: For DAS-managed information systems, configuration management development and implementation responsibilities shall be under the direction of the change control board or other entity as assigned by DAS OIT.

5.4 Security Impact Analysis (CM-4): DAS IT Operations personnel shall identify proposed changes to DAS-managed information systems that have a potential IT security impact and forward them to the IT security representative on the change control board for evaluation prior to implementation.

5.5 Verification of Security Functions (CM-4): DAS IT Operations personnel shall verify that approved changes to DAS-managed information systems are implemented correctly, operating as intended, and meeting security requirements.
5.6 **Access Restrictions for Change (CM-5):** Only authorized individuals shall be permitted to implement changes, upgrades and/or modifications to DAS-managed information systems.

5.6.1 Access control mechanisms shall be employed as outlined in NIST SP 800-53.

5.6.2 DAS OISP Governance, Risk, and Compliance personnel shall conduct compliance monitoring to identify unauthorized changes.

5.6.3 DAS-managed information systems with high or moderate criticality or confidentiality data classification ratings shall be audited annually. DAS-managed information systems with low criticality or confidentiality data classification ratings shall be audited every two years. Refer to Ohio Administrative Policy IT-13, “Data Classification”, for additional rating guidance.

5.6.4 Application developers shall be prohibited from having access rights to implement changes or modifications to DAS-managed information system production environments unless an exception is approved by DAS OISP.

5.6.5 Only authorized individuals shall have access to implement changes to software resident within software libraries for DAS-managed information systems.

5.7 **Least Functionality (CM-7):** DAS-managed information systems shall be configured to provide only essential capabilities and specifically prohibit the use of unnecessary functions, ports, protocols, services, and software.

5.7.1 Service owners shall review DAS-managed information systems periodically to identify and disable any unnecessary and non-secure functions, ports, protocols and services.

5.7.2 Service owners shall maintain a list of implemented functions, ports, protocols and services used in DAS-managed information systems.

5.7.3 DAS-managed information systems shall employ a deny-all, allow-by-exception policy.

5.8 **DAS-managed Information System Component Inventory (CM-8):** The DAS Office of Information Technology (OIT) shall maintain an accurate inventory of components within the **authorization boundary** of the DAS-managed information system.
5.8.1 All configuration items identified and placed under configuration management shall be populated and maintained in the state’s Configuration Management Database (CMDB). Configuration items shall be current, accurate, and complete; and their relationships to other configuration items maintained appropriately throughout the lifecycle of the configuration item.

5.8.2 Automated mechanisms shall be leveraged, whenever possible, to detect the introduction of unauthorized components into the DAS-managed information system, disable network access by such components, and notify DAS OISP personnel of the unauthorized access.

5.8.3 An inventory of components along with a list of personnel responsible for administering the components shall be maintained.

5.8.4 Currently deployed component configurations, with approved deviations, shall be included in the DAS-managed information system component inventory.

5.9 Configuration Management Plan (CM-9): Service owners shall establish a configuration management plan for DAS-managed information systems that aligns with their change management process. Configuration management plans shall be maintained by operations personnel, or other entity as assigned by DAS OIT, and shall address:

- Roles and responsibilities;
- Configuration management processes and procedures;
- A process for identifying, defining and managing configuration items;
- A procedure for placing configuration items under configuration management; and
- A procedure for conducting configuration audits.

6.0 PROCEDURES

6.1 Exception Process: To request an exception to one or more of the requirements outlined in this policy, please complete an IT Security Exception Request form.

6.1.1 The form is located within the IT Enterprise Services Portal under the “Services & Products” category.

6.1.2 If you have any questions, please contact DAS OISP (refer to Section 9.0 Inquiries for contact information).
7.0 COMPLIANCE

To assist DAS entities with meeting the configuration management requirements outlined in the policy, a general implementation framework includes:

7.1 The configuration management requirements for existing DAS-managed information systems with high or moderate criticality or confidentiality data classification ratings shall be implemented within six months from the original effective date of the policy, April 20, 2017.

7.2 The configuration management requirements for existing DAS-managed information systems with low criticality or confidentiality data classification ratings shall be implemented, if not already, within two years from the original effective date of the policy (April 20, 2017).

7.3 All planned and future DAS-managed information system development initiatives, shall immediately comply with the configuration management requirements outlined in this policy.

8.0 DEFINITIONS

Authorization Boundary - All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.\(^1\) Also commonly referred to as the information system boundary.

Availability - Ensuring timely and reliable access to and use of information.\(^2\)

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.\(^3\)

Configuration Management - A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.\(^4\)

DAS-managed Information System - Information systems that reside in facilities or infrastructure managed by DAS OIT personnel. Primary responsibility for managing these systems may be assigned to DAS OIT personnel or other outside entities.

\(^2\) Ibid.
\(^3\) Ibid.
Data Owners – The data owner is responsible for the identification and classification of information, in consultation with Legal Counsel, and shall address the assignment of data classification labels, data compilation, data classification coordination, data classification compliance and data access. The role of a data owner and his/her associated responsibilities are addressed in detail within Ohio Administrative Policy IT-13, “Data Classification.”

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (E.g., servers, workstations, networking components).

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Least Functionality - Devices are configured to allow only the necessary ports, protocols, and services in accordance with functional needs and the risk tolerance in the organization. Open ports and available protocols and services are an inviting target for attackers, especially if there are known vulnerabilities associated with a given port, protocol, or service.

Malicious Code - Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Some examples include a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Ports - Ports are logical addresses on a computer that allow communication using various protocols, such as FTP. Ports used in this context should not be confused with the physical serial and parallel ports used for devices such as printers, scanners and the mouse.

Protocol - A set of rules for assembling and transmitting data over a network.

Security Impact Analysis - The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

---

6 Ibid.
9 Ibid.
Services - The application of business and technical expertise to enable organizations in the creation, management and optimization of or access to information and business processes.

Service Owner – A service owner is responsible for the delivery (design, performance, and integration), continual improvement and management of assigned IT services.

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.  

9.0 INQUIRIES

Direct inquiries about this policy to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor

1.614.644.9391 | state.isp@das.ohio.gov

DAS Policies may be found online at http://www.das.ohio.gov/Divisions/Administrative-Support/Employees-Services/DAS-Policies

Additional information regarding the Office of Information Security & Privacy may be found online at InfoSec.Ohio.Gov.

10.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/20/2017</td>
<td>Original Policy</td>
</tr>
<tr>
<td>06/18/2018</td>
<td>Updated the policy to include additional change and configuration management requirements.</td>
</tr>
<tr>
<td>12/21/2018</td>
<td>Review of established baselines frequency updated. The exception request language was also modified to align with the current procedure.</td>
</tr>
<tr>
<td>12/21/2019</td>
<td>Scheduled policy review.</td>
</tr>
</tbody>
</table>

11.0 ATTACHMENTS

None.

---