System and Communications Protection Policy

<table>
<thead>
<tr>
<th>POLICY NUMBER:</th>
<th>EFFECTIVE DATE:</th>
<th>APPOINTING AUTHORITY APPROVAL:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2100-21</td>
<td>01/15/2020</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REPLACES POLICY DATED:</th>
<th>AUTHORITY:</th>
<th></th>
</tr>
</thead>
</table>

1.0 PURPOSE

This policy establishes the system and communications protection requirements for managing risks and establishes a system and communications protection program. The system and communications protection program helps DAS implement security controls with regard to system configuration and data communication and transfer.

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 and Technology (NIST) Special Publication (SP) 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” family identifiers and control numbers are provided in parentheticals next to requirement headers, where applicable.

2.0 SCOPE

The scope of this policy covers any DAS-managed system assets, including system assets managed by external service partners.

3.0 BACKGROUND

The security risks associated with information technology are always increasing in both number, variety, and severity. Attacker sophistication and capabilities improve every day. These ongoing threats create a challenging environment in which to protect and safeguard DAS information systems.

Mitigating against these threats requires a multilayered approach and coordination between a variety of agency resources, including security professionals, system and service owners. This policy defines the controls that need to be in place to help protect systems and communications. The requirements address a number of security controls for mitigating risks from vulnerable system configuration and data communication and transfer.
4.0 REFERENCES

4.1 NIST 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.

5.0 POLICY

The following system and communications protection controls shall be applied to DAS-managed system assets, including those managed by external service partners:

5.1 Application Partitioning (SC-2): The information system shall separate user functionality from information system management functionality. The separation can be either physical or logical, and implemented by using different computers, different central processing units, different instances of operating systems, different network addresses, different web interfaces, virtualization techniques, or combinations of these or other methods, as appropriate.

5.2 Information in Shared Resources (SC-4): The information system shall prevent unauthorized and unintended information transfers via shared system resources. This control is commonly referred to as object reuse and residual information protection. Information, including encrypted information, of previous users, roles, or processes in shared systems resources (e.g. registers, main memory, hard disks) is prevented from being available to any current users, roles, or processes after those resources have been released back to the information system.

5.3 Denial of Service Protection (SC-5): The information system shall be protected against or able to limit the effects of denial of service (DoS), including distributed denial of service (DDoS), attacks. For example, boundary protection devices can filter certain types of packets to safeguard information systems on internal networks from DoS and DDoS attacks.

5.4 Boundary Protection (SC-7): The information system shall:

- Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;
- Implement subnetworks for publicly accessible systems that are physically or logically separated from internal networks. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs); and
- Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices (e.g. routers, gateways, firewalls) based on a security architecture.
5.4.1 **Access Points**: The information system shall limit the number of external network connections. Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic.

5.4.2 **External Telecommunications Services**: Each external telecommunication service shall have a managed interface with a traffic flow policy to protect the confidentiality and integrity of the information being transmitted.

5.4.3 **Deny by Default and Allow by Exception**: The information system at managed interfaces shall deny network communications traffic by default and allow network communications traffic by exception. A deny all and permit by exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

5.4.4 **Prevent Split Tunneling for Remote Devices**: The information system in conjunction with a remote device shall prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. VPNs shall be considered non-remote connections and split tunneling is prohibited.

5.5 **Transmission Confidentiality and Integrity (SC-8)**: The information system shall protect the confidentiality and integrity of transmitted information. This can be accomplished by physical means (e.g., employing protected distribution systems) or by logical means (e.g., employing encryption techniques).

5.5.1 **Cryptographic or Alternate Physical Protection**: The information system shall implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless protected by alternate physical safeguards.

5.6 **Network Disconnect (SC-10)**: The information system shall terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity. This control applies to both internal and external network connections.

5.7 **Cryptographic Key Establishment and Management (SC-12)**: Cryptographic key management and establishment shall be performed using manual procedures or automated mechanisms with supporting manual procedures. Trust stores are to be managed to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to the information systems and certificates related to the internal operations of systems.
5.8 **Cryptographic Protection (SC-13):** The information system shall implement cryptographic protection in accordance with Ohio IT Standard ITS-SEC-01, “Data Encryption and Cryptography,” and with applicable federal and state laws, executive orders/directives, regulations, policies, and standards.

5.9 **Collaborative Computing Devices (SC-15):** The information system shall prohibit remote activation of collaborative computing devices (e.g., networked white boards, cameras, and microphones), and provide explicit indication of use, (e.g., signals to users when collaborative computing devices are activated) to users physically present at the devices.

5.10 **Public Key Infrastructure Certificates (SC-17):** Public key infrastructure certificates shall be issued by the DAS certificate authority (CA) or obtained from an approved service provider.

5.11 **Mobile Code (SC-18):** DAS OISP shall define acceptable and unacceptable mobile code and mobile code technologies, establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies, and authorize, monitor, and control the use of mobile code within the information system. Decisions regarding the use of mobile code within the information system are based on the potential to cause damage to the system if used maliciously.

5.12 **Voice over Internet Protocol (SC-19):** DAS OIT shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies and authorize, monitor, and control the use of VoIP within the information system. Decisions regarding the use of VoIP within the information system are based on the potential to cause damage to the system if used maliciously.

5.13 **Secure Name and Address Resolution Service (SC-20 and SC-21):** The information system shall:

- Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name and address resolution queries;
- Provide the means to indicate the security status of child zones (if the child supports secure resolution services) and to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace; and
- Request and perform data origin authentication and data integrity verification on the name and address resolution responses the system receives from authoritative sources.
5.14 Architecture and Provisioning for Name and Address Resolution Service (SC-22): The information system that collectively provides the name and address resolution service shall be fault-tolerant and implement internal and external role separation. To eliminate single points of failure and enhance redundancy, employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. For role separation, DNS servers with internal roles shall only process name and address resolution information requests from internal clients and DNS servers with external roles from external clients.

5.15 Session Authenticity (SC-23): The information system shall protect the authenticity of communications sessions. This control addresses communications protection at the session level, versus packet level, and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into sessions.

5.16 Protection of Information at Rest (SC-28): The information system shall protect the confidentiality and integrity of user and system information at rest. Information at rest refers to the state of information when it is located on storage devices in specific components of information systems. System information requiring protection includes configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content.

5.17 Process Isolation (SC-39): The information system shall maintain a separate domain for each executing process. Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that one process cannot modify the executing code of another process and communication between processes is performed in a controlled manner through security functions. This capability is available in most commercial operating systems that employ multi-state processor technologies.

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 system and communication protection requirements outlined in the policy, a general implementation framework includes:

7.1 All existing DAS information systems shall comply with the system and communication protection requirements within one year from the effective date of the policy.

7.2 All planned and future DAS information system development initiatives shall immediately comply with the requirements outlined in this policy.

8.0 DEFINITIONS

**Boundary Protection Devices** – A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.¹

**Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.²

**DAS-managed System Asset** - Information, hardware, software and services required to support state business, and identified during the risk assessment process as assets that need to be protected. Primary responsibility for managing these system assets may be assigned to DAS OIT personnel or other outside entities.

**Denial of Service (DoS)** - The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)³

**Distributed Denial of Service (DDoS)** - A Denial of Service technique that uses numerous hosts to perform the attack.⁴

**Firewall** – A device or program that controls the flow of network traffic between networks or

---


² Ibid.


hosts that employ differing security postures.\(^5\)

**Gateway** – An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.\(^6\)

**Information System Management Functionality** – Functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.\(^7\)

**Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.\(^8\)

**Mobile Code** - Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.\(^9\)

**Protected Distribution Systems** – Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.\(^10\)

**Public Key Infrastructure** - The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.\(^11\)

**Router** – On a network, a device that determines the best path for forwarding a data packet toward its destination. The router is connected to at least two networks, and is located at

---


\(^8\) Ibid.

\(^9\) Ibid.


the gateway where one network meets another.\(^\text{12}\)

**Split Tunneling** – A method that routes organization-specific traffic through the SSL VPN tunnel, but routes other traffic through the remote user's default gateway.\(^\text{13}\)

**Trust Anchors** – A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate). A trust anchor may have name or policy constraints limiting its scope.\(^\text{14}\)

**Trust Stores** - Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.\(^\text{15}\)

**Voice over Internet Protocol** - Voice over IP (VoIP, abbreviation of voice over Internet Protocol) is a methodology and broad range of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

### 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 https://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 of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/15/2020</td>
<td>Original Policy.</td>
</tr>
<tr>
<td>01/15/2021</td>
<td>Scheduled Policy Review.</td>
</tr>
</tbody>
</table>

11.0 ATTACHMENTS

None.