P.02

Policy Name

Architecture and Network Security Policy

1. Purpose

The purpose of this Policy is to establish rules for the secure management, configuration, and use of State network infrastructure, including secure architecture. Consistent, secure networking and architecture implementation practices help to preserve the confidentiality, integrity, and availability of the State Enterprise.

2. Scope

The Statewide IT Policies and Standards ("POLICIES") apply to all IOT-supported entities ("Entities"), their employees, their contractors, their consultants, and their vendors. Unless otherwise specified, all of the POLICIES apply equally to physical and electronic assets and resources assigned to an individual, on-premises physical assets, on-premises virtual assets, on-premises cloud assets, assets provided by cloud service providers, products and/or services that use cloud computing, all data stored or processed by the above assets in electronic, paper, or any other form, and everything else that supports the functioning of State government ("State Enterprise").

3. Policy

3.1. Enterprise Network Requirements

a. IOT and Entities with responsibility for supporting infrastructure must select and support industry-standard, secure, and nondeprecated networking protocols. These protocols should be updated and evaluated as new standards become available.
b. Networks should be properly segmented based on purpose and function (i.e., networks facing the public internet or other internal networks with varying degrees of critical data). This should be accomplished using routers, firewalls, and other secure, industry-standard network segmentation techniques for the physical and logical separation of networks.
c. In the event of a security breach, Entities should consider existing network architecture as a mechanism to contain the breach or security event.
d. Hardening techniques and other vendor-provided controls for securing network devices must be used to strengthen overall security and reduce unauthorized access.
e. The principle of least privilege must be considered when assigning network access. This should include securing and monitoring user authentication.
f. Administrative credentials with elevated privileges (i.e., access to the management network) should use privilege access accounts and include protections such as password complexity requirements, salting and hashing, and multifactor authentication.
g. All new information systems and applications must have encryption applied to both inbound and outbound data traversing the network in accordance with the Encryption and Cryptography Policy, the Encryption and Cryptography Standard, and associated guidelines. Legacy systems and applications should be evaluated by their owners for compliance.
h. Redundancy should be considered wherever possible (e.g., redundant links, switches, routers, firewalls).
i. IOT and Entities must maintain and update a list of countries that present increased risk, including risk in information transmissions or in business relationships. The list of countries may include countries with which interaction is prohibited, countries with which interaction is allowed under certain conditions, and other categories. (Please see the Indiana Department of Administration for information regarding the creation of business relationships with entities in foreign jurisdictions.)

3.2. Firewall Use

a. IOT should deploy firewalls and other tools designed to prevent horizontal movement where IOT concludes that it is necessary.
b. Entities must use IOT-provided firewalls. If an Entity has previously deployed a firewall, it must submit an Exception Request.
c. Every connection between the State network and other external entities should be brokered using a firewall.
d. External internet traffic should flow through a load balancer.

e. Egress filtering, or the filtering of outbound traffic, should be performed wherever possible.
f. Firewalls must be hardened and locked down, running only the minimum required services.
g. Firewalls must log all security-relevant traffic originating from untrusted networks, including both ingress and egress traffic.

3.3. Wireless Networks

a. Wireless networks must be accessed in accordance with the End User Internet Use Standard. This includes any Statewide POLICIES, guidelines, or procedures for visitors or guests accessing IOT-supported wireless networks.
b. An inventory of authorized wireless access points should be maintained. Users must not implement or use unapproved network access points. IOT networking and security teams reserve the right to detect and remove any unauthorized access points from the network.
c. IOT and Entities should take action to identify and address unauthorized devices on the network.
d. The default vendor settings on all wireless devices must be changed, including, but not limited to, default wireless encryption keys and passwords.

3.4. Management and Periodic Review

a. To ensure hardware integrity, network devices and associated hardware should only be purchased from authorized manufacturers and value-added resellers ("VAR"s), via state-approved procurement methods.
b. Network personnel and administrators should receive regular training on security best practices as it relates to configuration and maintenance of enterprise networks.
c. Security configurations should be tested annually against established network security requirements. Testing may include penetration tests, internal audits, and validation against a secure baseline.
d. Architectural changes to networks, including the addition of new infrastructure or major configuration changes, should be documented and available prior to engagement with information security architecture leadership.

3.5. International Work

"International Work" and "Abroad" are synonymous. Each means State of Indiana business or work outside the contiguous 48 states and the District of Columbia, regardless of why the individual is Abroad. Any other location is international or has a likelihood of placing data on non-U.S. information systems. Please see International Work Standard.

4. Exceptions

Exception Requests will be addressed through the process designated by IOT.

5. Ultimate Authority

The Chief Information Officer is the ultimate authority for decisions made pursuant to the POLICIES, including Exception Requests.

6. Roles and Responsibilities

State agencies vary tremendously. Some State agencies have Chief Information Officers, while others may have no dedicated IT employees. Because of that variance, the Statewide IT Policies and Standards do not refer to a specific job title as being responsible for compliance. Instead, the intent is for the responsibilities to rest with the agency head or the highest-ranking employee responsible for IT, unless stated otherwise regarding a specific duty.

7. Statutory Purposes

The statutory purposes of IOT include "establish the standards for the technology infrastructure of the state" and "provide for the technology and procedures for the state to do business with the greatest security possible," Ind. Code § 4-13.1-2-1(1) and (5). IOT has an obligation to "develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government," Ind. Code § 4-13.1-2-2(a)(11).

8. Industry Standards

The Statewide IT Policies and Standards are based on the following:

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, U.S. National Institute of Standards and Technology, Special Publication 800-37 Rev. 2. https://csrc.nist.gov/pubs/sp/800/37/r2/final

Security and Privacy Controls for Information Systems and Organizations, U.S. National Institute of Standards and Technology, Special Publication 800-53 Rev. 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Critical Security Controls v.8.1, Center for Internet Security. https://www.cisecurity.org/controls

9. Federal Audit

The federal government audits the IT practices of several Entities. Where necessary, those Entities may create agency-specific policies to supplement the Statewide IT Policies and Standards. Those agencies include the Bureau of Motor Vehicles, Department of Child Services, Department of Revenue, Department of Workforce Development, Family and Social Services Administration, Indiana Office of Technology, and the Indiana State Police.