State of Indiana Information Security Framework

P.01

Policy Name

Acceptable Use Policy

1. Purpose

This Policy establishes how individuals are to use and protect the State's Information Technology Resources. The requirements outlined in this Policy are designed to minimize potential damage that may result from the unacceptable use 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 Information Technology Resources User Policy and Agreement

a. IOT must maintain an Information Technology Resources User Policy and Agreement ("User Policy") to correspond with this Policy.
b. All individuals using state resources are responsible for reading and abiding by the requirements of the User Policy.
c. The User Policy must cover topics related to the expectations of end users and the acceptable use of technology resources, including State-provided hardware, data, and any other applicable resources.
d. The User Policy should be reviewed annually.
e. Individuals performing State of Indiana business must receive information security awareness training as defined in the Security Awareness and Training Policy.
f. The User Policy must be available to users upon request or in a publicly accessible location.
g. The User Policy should align with the POLICIES.
h. The User Policy may not address every information security issue or scenario. Some situations may require employees to exercise critical judgment. If an uncertain situation arises, users should seek guidance from the IOT Security Team.

3.2 Acceptable Use of Information Resources

An individual using something in the State Enterprise is required to:

a. Protect the State Enterprise.
b. Comply with the POLICIES.
c. Use only authorized devices to access the State Enterprise.
d. Protect their accounts with a password. An individual may not share the password. An individual should use the IOT-provided password manager.
e. Use their own credentials to access the State Enterprise and comply with all authentication and access control policies and procedures.
f. Report any suspected breaches or security incidents via established incident reporting mechanisms. See Incident Response and Outage Response Policy.
g. All hardware and software provided to an individual remain the sole property of the State and must be returned to IOT:
    i. Before the individual's termination of state employment, or
    ii. Before the individual's transfer to a different Entity.
h. All hardware and software provided to an individual for International Work must be returned to IOT:
    i. Immediately after the International Work, and
    ii. Without having been reconnected to the State network.

"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.

i. An individual is responsible for storing physical parts of the State Enterprise in a safe and secure place.
j. An individual must take appropriate action to protect the State Enterprise from damage or theft, including when working at remote locations.
k. An individual must return State of Indiana property to IOT and in a reasonable condition, without significant damage.
l. Using a State of Indiana resource outside the contiguous 48 states and the District of Columbia is prohibited.

3.3 Email System

a. The primary purpose of email is for professional, job-related communications.
b. The email system may not be used for sending inappropriate or offensive items.
c. The email system may not be used for broadcasting a message for personal or malicious use, including announcements, commentary, or advertisements of any kind.
d. Email should not be used to send large attachments that can cause significant disruptions to email services. IOT may establish a maximum size for email attachments.
e. Sending emails in a manner that masks the individual's identity or makes it appear that the message came from a different sender (forging, altering, or removing email headers) is prohibited.
f. An individual must use extreme caution when opening unsolicited email and attachments, which may contain a Cybersecurity Risk. An individual must contact the help desk if in doubt about the safety of an email.

3.4 Monitoring

a. An individual must be aware that the data they create on State-owned systems remain the property of the State. Because of the need to protect the State Enterprise, an individual does not have a reasonable expectation of privacy in their use of the State Enterprise.
b. For security and network maintenance purposes, authorized individuals within IOT may monitor equipment, systems, and network traffic at any time. Monitoring includes, but is not limited to, software applications, email, Voice over Internet Protocol ("VoIP"), telephone calls, and web browsing. IOT reserves the right to disclose evidence of misconduct or other criminal wrongdoing to appropriate authorities, including law enforcement entities. Such reports will be made in accordance with applicable law and policy.
c. IOT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Policy.

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.

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.

P.03

Policy Name

Asset Management Policy

1. Purpose

The purpose of this Policy is to define the requirements for managing hardware, software, and third-party cloud applications. This Policy also provides a framework for IOT-supported entities to perform Asset management services supplemental to those provided by IOT.

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 Definitions

a. "Asset" means hardware, software, firmware, cloud resources, or any other tool deployed to support the State's information systems.

b. “Asset Inventory” means the inventory identified by IOT.
c. “Hardware” means a type of Asset that includes servers, data center resources, workstations, and other endpoints.
d. “Owner” means the person responsible for the Asset.

3.2 General Provisions and Asset Lifecycle Management

a. An Entity must neither procure nor deploy an Asset other than one authorized by IOT.
b. Upon a person’s termination of state service, three-month leave, or transfer to a different Entity, an Entity must return to IOT all Assets assigned to that person, including all workstations, cell phones, tablets, identification badges, and any other tools used for identification, access, or encryption.
c. IOT must reimage an Asset before reissuing it.
d. The Asset lifecycle includes, but is not limited to, each of the following:
    i. Acquisition
    ii. Receipt
    iii. Deployment
    iv. Maintenance
    v. Physical and virtual location
    vi. Destruction
e. Where applicable, the lifecycle will also include:
    i. The person to whom the Asset is assigned
    ii. Contact information for the assigned person
f. IOT and Entities must maintain accurate and updated information regarding Assets in the Asset Inventory and throughout the Asset lifecycle. IOT and Entities must annually review and update this information.
    i. The Asset Inventory should integrate information from several information systems, including procurement, billing, shipping, configuration, and destruction.
    ii. IOT will configure the Asset Inventory to require certain information, which will vary depending on the type of Asset. The Asset Inventory should include the Asset’s Owner, details on its connection to the network, and its criticality.

3.3 Hardware

a. All Hardware above $500 in value must have an Owner.
b. Hardware must have a mechanism for identification to enable accurate tracking and management. This may be implemented through Asset tags.
c. All new Hardware must be approved and reviewed before it can be allowed on the network.
d. IOT will provide tools for identifying, scanning, patching, updating, and logging Assets, and centrally managing Asset control.
    i. An Entity must ensure that its Assets are powered and connected to the State of Indiana network or to internet service at least every three months.
    ii. Neither an Entity nor a person may disable a tool deployed for any of the above-named purposes.
e. IOT and Entities will designate approved individuals to ship Assets to office spaces and other facilities used for State of Indiana business. Shipping Assets to a residence is prohibited.
f. Owners are responsible for ensuring that all assigned Assets remain within vendor support. When seeking extended support, an Entity must use the IOT-approved extended support vendors.
g. IOT and Entities must maintain a warranty on all servers. Procuring an extended warranty is required when an Asset is no longer covered by the initial plan.
h. IOT will assign a unique identifier to each hard drive and maintain proof of destruction for all drives. IOT will enforce the sanitization of cloud-hosted data through the use of contractual language and verification processes, depending on the specific cloud vendor.
i. IOT will manage the process by which workstations are refreshed and upgraded.
j. The Asset Inventory should provide categorizations based on the business use and the environment in which the Hardware will be used. Categorizations must allow for the prioritization of Assets.
k. Assets must be destroyed using IOT’s approved methods. The destruction of an Asset requires a ticket documenting the Asset’s destruction.
l. IOT should perform periodic scanning for rogue wireless access points.
m. Appropriate diagrams depicting relevant electronic communications and data flows between Assets must be maintained and reviewed by IOT for accuracy at least annually, or upon significant changes to the environment.

3.4 Software, External, and Cloud Assets

a. All software and cloud Assets must have an Owner.
b. Software and cloud Asset inventories must be reviewed at a defined interval to ensure that listings are accurate, and licensing is up to date. Inventories should include a categorization based on business use and the environment in which the software or cloud Asset is used.

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.

P.04

Policy Name

Configuration Management Policy

1. Purpose

The purpose of this Policy is to provide assurance that the systems and assets in the State Enterprise are systematically controlled and that

accurate and reliable information about those systems, assets, and their associated configurations is available when needed.

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 Configuration Management

a. IOT must establish and maintain a secure configuration process for enterprise assets (e.g., endpoints, network infrastructure, cloud assets, storage arrays, servers).
b. IOT and Entities should harden systems and assets according to industry security standards and manufacturer recommendations.
c. IOT and Entities should maintain records of configuration settings within the associated secure configurations guidelines and, where available, the associated Configuration Management Database ("CMDB"). IOT should review this information annually and update it when necessary.
d. IOT and Entities should list all systems and assets in the CMBD, including network and cloud assets.

3.2 Baseline Configuration

a. Hardened baseline configurations should provide a commensurate level of security in alignment with the specific asset or system criticality rating.
b. IOT and Entities must apply hardened baseline configurations to systems and assets before connecting to the State network.
c. IOT and Entities should use secure, nondeprecated network management protocols, such as Secure Shell ("SSH"), Hypertext Transfer Protocol Secure ("HTTPS"), and a nondeprecated version of Transport Layer Security ("TLS") to manage enterprise assets and software.
d. Assets hosting sensitive data should require additional security controls (e.g., penetration tests, static code analysis) as part of the initial platform development.
e. IOT and Entities should follow least privilege in selecting configuration settings by allowing users to have only those capabilities necessary for their roles, including the disabling of unnecessary services.
f. IOT and Entities should establish, document, implement, and monitor mandatory configuration settings for assets using a security configuration checklist that reflects the most restrictive mode, consistent with operational requirements.
g. IOT and Entities must configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed fifteen minutes. For mobile enduser devices, the period must not exceed two minutes.
h. IOT and Entities should enforce automatic device lockout following a predetermined threshold of local, failed authentication attempts on portable end-user devices. For laptops, do not allow more than twenty failed authentication attempts. For tablets and smartphones, do not allow more than ten failed authentication attempts.
i. IOT and Entities should include the capacity of remotely wiping portable end-user devices.

3.3 Applying Configuration Settings

a. IOT must establish and document a golden image or secure build of systems and assets for workstations, servers, and network equipment. This should include trusted or enterprise-controlled Domain Name System ("DNS") servers.
b. To protect the integrity of the image, golden images should be stored in a secure location that is only accessible by individuals with a business need.
c. All purchased, vendor-configured systems must have appropriate configuration documentation, including baseline configuration details when possible.
d. Asset configuration privileges should be limited to administrators with valid authority.

e. IOT must account for default manufacturer settings and accounts and change default credentials.

3.4 Applying Cloud Configuration Settings

a. When applicable and feasible, a baseline image must be established for cloud resources and infrastructure.
b. Configuration settings and changes related to cloud infrastructure and assets (e.g., compute, network, and storage) must be evaluated based on State and Federal requirements.
c. Cloud configuration management must follow the benchmarks required by the cloud service provider based on the shared responsibility model.

3.5 Change Control and Plan Management

a. Configuration changes must be documented and approved as part of the change management process prior to implementation. See the Change Management Policy for more information.
b. IOT and Entities should maintain previous configurations to support a secure rollback.

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.

P.05

Policy Name

Indiana Risk and Authorization Management Program (RAMP) Policy for Cloud Offerings

1. Purpose

Risk and authorization management programs – or "RAMPs" – are intended to protect data and technology resources while making the process of contracting for cloud offerings more straightforward, predictable, objective, and uniform. They achieve this by setting basic requirements for security assessments, authorizations, continuous monitoring, and other necessary components of cloud contracts that cloud providers are expected to meet. The requirements are based on generally accepted industry standards and are established in the form of minimum security-level matrices with different security controls that are based on the data and infrastructure involved and the impact of their potential loss or disruption. FedRAMP, the federal government's RAMP, is one example. The purpose of this policy is to create a RAMP for the State of Indiana.

2. Scope

This policy applies to all executive branch state agencies, departments, institutions, and similar entities that are responsible to the Governor of the State of Indiana. It also applies to any other entities that utilize, integrate with, or are otherwise connected to the State's systems, network, or other IT infrastructure. All such entities are covered by the scope of this policy, and all such "covered entities" must abide by its requirements – for any contracts for cloud offerings which are executed, amended, or renewed on or after October 14, 2025 – because of our collective need to protect data and the technology resources that are used to store, process, and transmit it.

3. Policy

3.1 Definitions

a. "Cloud offerings" are on-demand software applications, virtualized computing hardware (such as servers, storage, networks, and other infrastructure), or entire platforms for managing these resources that are provided over the internet. These products are frequently sold as "subscriptions." In such cases, they are commonly referred to as "software as a service," "infrastructure as a service," "platform as a service," and the like. They may also be included as part of a service that is provided by a vendor – for example, when an agency procures commercial off-the-shelf offerings from a third-party reseller or uses a vendor to develop and build systems outside of IOT's data centers and tenants. In most cases, the use of cloud offerings results in data being maintained remotely on servers, in data centers, or on other infrastructure that is not located within a state-owned datacenter or IOT-managed infrastructure or cloud tenants.
b. "Covered entities" are executive branch state agencies, departments, institutions, and similar entities that are responsible to the Governor of the State of Indiana as well as any other entities that utilize or are otherwise connected to the State of Indiana's systems, network, and other IT infrastructure.
c. "Critical infrastructure," for the purposes of this policy, refers to the systems and assets that are vital for society's smooth and safe operation. They are resources that Hoosiers depend on daily, in one way or another. Some tangible, physical examples are roads, bridges, power plants, electrical grids, water treatment plants, communication networks, transportation networks, hospitals, banks, and essential government facilities. Some intangible, virtual examples are the internet and essential government services. Disruption to critical infrastructure can have severe consequences on society's economy, security, health, and general well-being.
d. "IOT" means the Indiana Office of Technology, the executive branch agency of the State of Indiana created by IC 4-13.1, or its designee.
e. "Maturity assessor" means an independent, nationally recognized, compliance authorization organization with multistate connections.
f. "Minimum security level matrices" are the two-part framework to be used for selecting the minimum verified security designation levels - also referred to as GovRAMP statuses - that are required for cloud offerings, based on the data and infrastructure involved and the impact of their potential loss or disruption. There are three different levels in the matrices: GovRAMP Core, GovRAMP Authorized, and GovRAMP Authorized + CJIS Overlay. Each level calls for different NIST 800-53 controls to be in place. The minimum security level matrices are available, below, in Appendix 1.

3.2 Requirements

a. Cloud offerings must not be procured, otherwise obtained, or used unless they have been approved by IOT.

b. Proposed solicitations for cloud offerings must be provided to IOT no less than 90 days prior to the anticipated release to potential cloud providers for bidding, so that they can be meaningfully reviewed and approved.
c. Cloud offerings must:
    i. Comply with the NIST 800-53 controls that are necessary to meet the minimum security designation levels, which are called for by the minimum security level matrices in Appendix 1, by a reasonable date certain from the date on which they are procured, otherwise obtained, or used by a covered entity, not to exceed 18 months of the effective date of the resulting contract or one-half its term, whichever is shorter;
    ii. Continue to meet the necessary levels throughout the term of the contract, as determined by a maturity assessor, with evidence of the same being provided to covered entities and IOT on no less than a quarterly basis; and
    iii. Have regular risk assessments and continuous monitoring conducted on them, by a maturity assessor, throughout the term of the contract.
d. Contracts for cloud offerings must include language by which cloud providers agree to the requirements of Section 3.2.c, above.

4. Exceptions

The requirements of this policy are the default standards for 100+ state agencies, departments, institutions, and similar entities that are responsible to the Governor of the State of Indiana, as well as any other entities that utilize the State's systems, network, or other IT infrastructure. They are intended to protect the data of these different entities and the technology resources that are used to store, process, and transmit it. The minimum security level matrices that are discussed in this policy are based on generally accepted industry standards that cloud providers should be familiar with and amenable to.

In the rare case when a covered entity believes that an exception to the requirements of this policy are warranted for a particular contract that it wishes to enter into, the covered entity should be prepared to describe the cloud offering in question, how it will enable the covered entity to serve Hoosiers, how much it costs, and whether sensitive data and/or critical infrastructure is involved and the volume thereof. The covered entity should also be prepared to describe precisely how the requirements should be modified and why it believes the modifications are warranted under the circumstances, because it has concluded that the security risks associated with making them are outweighed by the benefits to the covered entity's business and mission. Lastly, before an exception request is submitted to IOT, it must be approved by the highest-ranking authority at the covered entity (executive director, commissioner, agency head, etc.), who must acknowledge that he or she has reviewed the modifications and believes 4 an exception is warranted because the benefits to the covered entity's business and mission are judged to outweigh any associated security risks.

Exception requests must be submitted by means of IOT's electronic form, which is available via request at IOTContractExceptions@iot.in.gov.

5. Ultimate Authority

Executive Order 25-19 specifically directs IOT to create a RAMP policy like this one for the State of Indiana. IOT is also statutorily authorized by IC 4-13.1-2-1 and -2 to establish technology and cybersecurity policies for the State.

6. Roles and Responsibilities

a. The role of covered entities, regarding the cloud offerings that are discussed in this policy, is to act as the frontline protector of data and the technology resources that are used to store, process, and transmit it. Specifically, covered entities are responsible for:
    i. Ensuring that they do not procure, otherwise obtain, or use cloud offerings that have not been approved by IOT;
    ii. Providing solicitations for cloud offerings to IOT, no less than 90 days prior to the anticipated date of release, so that they can be meaningfully reviewed and approved prior to release;
    iii. Identifying and selecting the minimum security designation levels for cloud offerings that are called for in the minimum security level matrices in Appendix 1;
    iv. Including language in their contracts calling for their cloud providers to agree to the requirements of Section 3.2.c, above; and
    v. Receiving and reviewing evidence that their cloud offerings continue to meet minimum security designation levels on no less than a quarterly basis throughout the term of the contract; notifying IOT via email to IndianaRAMP@iot.in.gov that their cloud offerings no longer meet minimum levels when applicable and within 30 days of learning of the same; and conferring with cloud providers to determine whether the failure to meet minimum levels can be resolved within timeframes that are acceptable to both the covered entities in question and IOT.

b. The role of IOT is to be a second-line evaluator of the decisions that covered entities make with regard to cloud offerings and the contracts that they desire to enter into with cloud providers. Specifically, IOT is responsible for:
    i. Reviewing solicitations for cloud offerings that have been provided by covered entities;
    ii. Reviewing the minimum security designation levels that have been identified and selected by covered entities for cloud offerings and considering whether they are appropriate;
    iii. Reviewing contracts for cloud offerings to ensure that they include language calling for cloud providers to agree to the requirements of Section 4.c, above;
    iv. Receiving and reviewing email notices from covered entities regarding the failure of cloud offerings to continue to meet minimum levels, conferring with covered entities to determine whether the failure can be resolved within a timeframe that is acceptable to IOT, and informing the covered entities in question and the Indiana Department of Administration that contracts are to be terminated in those cases where the failure cannot be resolved within timeframes that are acceptable to IOT.

7. Statutory Purposes

This policy furthers the purposes identified in IC 4-13.1-2-1.

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.

Appendix 1

RAMP Minimum Security Level Matrices: *Data Type and Critical Infrastructure*

This appendix contains the two security requirement level matrices that covered entities are to use to identify and select the minimum security level for their cloud offerings. Matrix 1 pertains to “data type.” It requires covered entities to consider what type of data will be processed, stored, or transmitted by their cloud offerings. Matrix 2 pertains to “critical infrastructure.” It requires covered entities to consider whether critical infrastructure is supported in any way by their cloud offerings. Covered entities need to use both matrices to ensure that they identify and select the appropriate minimum verified security designation level or “GovRAMP Status.”

To use Matrix 1, covered entities should first look at Column 1 and determine what “data type” will be processed, stored, or transmitted by the cloud offering. There are three rows in Matrix 1 which correspond with the three different types of data for the purposes of this determination. Column 2 lists a handful of examples of various laws, regulations, and security policies that may apply to the three types of data listed in Column 1. The examples are provided for illustrative purposes only, in order to give covered entities an idea of the types of regulatory authorities that may apply to their data. Other authorities may also apply, however, and covered entities are expected to be familiar with the various authorities that apply to their particular data. Column 3 contains the corresponding data classification types discussed in Statewide IT Policy IOT-CS-SEC-102. It is included for internal cross-referencing purposes only. Lastly, covered entities should look to Column 4 to determine which minimum security designation level applies to their cloud offering

based on the data type in play: GovRAMP Core (which is the most basic level for nonconfidential data), GovRAMP Authorized (which contains additional requirements that are necessary to protect confidential data), or GovRAMP Authorized + CJIS Overlay (which contains even more requirements which are to protect CJIS Data). Each of those three levels require different NIST 800-53 controls to be in place. Additional information on GovRAMP statuses and the controls required for authorization under them can be found at https://govramp.org/providers/

Matrix 1			
1 - Data Type	**2 - Compliance/Regulatory Requirement**	**3 - Data Sensitivity Classification (per IOT-CS-SEC-102)**	**4 - Minimum Verified Security Designation Level Required (i.e GovRAMP Status)**
Data that is not required to be kept confidential by law, by contract, for business reasons, or for any other reason	NONE	Nonconfidential *or* Confidential - Proprietary	GovRAMP Core at the Moderate Impact level
Data that includes PII, PHI, FTI, PCI Data, SSA Data, education records, unemployment records, any other information that is required to be kept confidential by law, by contract, for business reasons, or for any other reason	Indiana Code, IRS Pub 1075, HIPAA, PCI, DSS, CMS, FISMA, 20 CFR 603, FERPA, others as applicable	Confidential - Sensitive *or* Confidential - Proprietary	GovRAMP Authorized at the Moderate Impact level
CJIS Data	CJIS Security Policy	Confidential - Sensitive *or* Confidential - Proprietary	GovRAMP Authorized + CJIS Overlay at the Moderate Impact level

To use Matrix 2, covered entities need to consider whether their cloud offerings will be used to support or could otherwise affect "critical infrastructure." For the purposes of this policy, "critical infrastructure" refers to the systems and assets that are vital for society's smooth and safe operation. They are resources that Hoosiers depend on daily, in one way or another. Some tangible, physical examples are roads, bridges, power plants, electrical grids, water treatment plants, communication networks, transportation networks, hospitals, banks, and essential government facilities. Some intangible, virtual examples are internet and essential government services. Disruption to critical infrastructure can have severe consequences impacting society's economy, security, health, and general well-being.

Matrix 2	
Critical Infrastructure?	**Minimum Verified Security Designation Level Required**
No	GovRAMP Core at the Moderate Impact level
Yes	GovRAMP Authorized at the Moderate Impact level

When covered entities determine that a higher minimum verified security designation level is required under one of the matrices than the other, they must select the higher level for their contracts. For example, if a covered entity determines that GovRAMP Core is required under Matrix 1 but GovRAMP Authorized is required under Matrix 2, it must select GovRAMP authorized. Covered entities

are always free to select higher levels for cloud offerings than is required by the matrices if they believe it makes sense to do so.

P.06

Policy Name

Data Classification and Management Policy

1. Purpose

The purpose of this Policy is to establish a comprehensive framework for categorizing and safeguarding data, including for purposes of cybersecurity and regulatory compliance.

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. Data Inventory, Data Flows, and General Protection Requirements

a. IOT must establish and maintain a data inventory that includes all sensitive data.
b. The data inventory must be reviewed and updated annually or when significant changes occur.
c. IOT and Entities must create data flow documentation for all systems, applications, and processes that involve the handling of sensitive data. These should be reviewed at least annually.
d. All individuals with access to, or who have responsibility for handling, data are required to undergo training in data protection and management.
e. IOT and Entities should implement processes that include data protection by design. "Data protection by design" refers to the integration of data protection considerations into the design and development of systems, processes, and services.

3.2. Data Retention and Disposal

a. IOT and Entities must limit the storage of data to that which is required for business, legal, and/or regulatory purposes. See Data Retention Standard.
b. Where possible, IOT and Entities should reduce the amount of data stored.
c. IOT and Entities must ensure that data disposal is conducted in accordance with a defined data retention schedule.

3.3. Data Classification

a. IOT should establish a Data Classification Standard including categories such as sensitive, confidential, and public.
b. Data classification categories must be reviewed and updated annually or when significant changes occur.

3.4 Data Loss Prevention

a. IOT must implement data loss prevention ("DLP") tools to identify all sensitive data stored, processed, or transmitted in the State Enterprise.
b. IOT and Entities should develop an inventory of sensitive data to be reviewed and updated annually, and/or upon significant change to the environment.

4. Exceptions

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.

P.07

Policy Name

Encryption and Cryptography Policy

1. Purpose

This Policy establishes the requirements for protecting IOT, agency, and citizen data while in transmission or at rest, both internally and externally. Sensitive data should be protected with administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability.

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 Encryption of Data in Transit

a. Sensitive information must be encrypted during transmission.
b. Transmission of data must be encrypted based on sensitivity level and State or Federal guidelines for secure data transmission. Please refer to the Data Classification Policy and Standard for further guidance.
c. All wireless connections must be encrypted. Please refer to the Encryption and Cryptography Standard for further guidance.
d. To connect to the network, an individual must be on an approved or sponsored device. Where permitted, individuals connecting to the network with a nonstate-provided device must connect through an encrypted connection.
e. Connections between IOT, Entities, and other providers, such as public cloud vendors, must be encrypted.

3.2 Encryption of Data at Rest

a. Data at rest must be encrypted. The Data Classification Standard outlines requirements for encryption based on sensitivity level.
b. Full disk encryption should be used when it is technically feasible and is the preferred method for encrypting software on databases and all data center infrastructure (e.g., servers, storage, and network).
c. IOT must provide disk encryption on all end-user devices.
d. All data stored or managed in cloud environments must be encrypted while at rest by the application managing the cloud environment. Regular reviews must be conducted to make sure that cloud environments follow all IOT encryption policies and standards.
e. Removable media are rarely permitted. All removable devices must be encrypted and use approved encryption algorithms outlined in the Encryption and Cryptography Standard.

3.3 Key Generation and Encryption Management

a. For all encryption referenced in this Policy, IOT and Entities must use secure, nondeprecated encryption algorithms. Please refer to the Encryption Standard for further guidance.
b. For all encryption referenced in this Policy, IOT and Entities must use only industry-standard encryption keys and industry-standard means of generating keys.
c. IOT must maintain physical and logical access control to key-generating tools and procedures. IOT must use least privilege in determining who may access the key-generating tools and procedures.
d. A documented key-rotation procedure and schedule must be implemented, including an annual rotation of master keys.
e. The use of any encryption or encryption tool other than that provided by IOT is prohibited.
f. Keys used for encrypting data at rest must be backed up following a documented and proven recovery process.

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.

P.08

Policy Name

Enterprise Resiliency Policy

1. Purpose

This Policy establishes requirements for maintaining the continuity of operations and establishing resilient business processes. This Policy also establishes a framework for ensuring proper emergency response and disaster recovery.

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 Business Continuity and Disaster Recovery Planning

a. IOT and Entities must have a documented Business Continuity Plan ("BCP") and an IT Disaster Recovery Plan ("DRP").
b. The BCP and DRP must be stored in multiple secure locations, ensuring their availability and resilience during disruptive events. At least one location must be non-digital.
c. Copies of the BCP and DRP must be distributed to key contingency personnel.
d. Plans must be updated and distributed to IOT and the Indiana Department of Homeland Security at defined intervals and in accordance with State requirements.
e. The BCP and DRP must be stored on-premises, off-premises, and in separate physical locations.

3.2 Developing and Implementing BCPs and DRPs

a. The BCP and DRP must address the required capacity to support critical missions and business functions, define recovery objectives and priorities, and identify roles and responsibilities.

b. Alternative storage and processing sites must be identified (permanent and/or temporary) at least 25 miles from the primary facility and configured with security measures equivalent to the primary site. IOT and Entities must establish the necessary third-party service agreements to allow for the resumption of information systems for operations of critical business functions within the time defined in the BCP or DRP (e.g., priority of service provisions).
c. Emergency power, backup telecommunications, and backup internet service must be available at the main site.
d. Alternate telecommunications and internet services must be established and sufficiently separated from the primary service provider.
e. The recovery and reconstitution of the information system, after a failure or other contingency, must be completed in a trusted, secure, and verifiable manner so that recovery can be validated.
f. IOT and Entities must identify critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to operations, staffing, materials, transport, facilities, and other aspects.
g. Business impact analyses should be used to evaluate the consequences of disasters, security failures, loss of service, and service availability.

3.3 Resiliency

a. Resiliency requirements to support the delivery of critical services must be established for all operating states (e.g., under duress/attack, during recovery, normal operations).
b. IOT and Entities must identify their place in critical infrastructure, specifically noting interconnections and integrations with other agencies, governments, and private organizations, where applicable.
c. Dependencies on critical functions must be established and considered when developing the BCP and DRP, including both internal and third-party-hosted systems.
d. Resiliency practices must be considered in the build and design of all information systems.
e. Information security requirements and considerations must be included and considered in all forms of resiliency planning.

3.4 Back-Up and Disaster Recovery

a. IOT must establish and maintain disaster recovery practices sufficient to restore enterprise assets to a pre-incident and trusted state.
b. IOT and Entities must perform backups weekly or more frequently, based on the sensitivity of the data.
c. Automated tools should be used to track the success of all backups.
d. The integrity and security of the backup copies must be maintained to ensure future availability. IOT should establish and maintain an isolated instance of all recovery data. Any potential accessibility problems with the backup copies must be identified and mitigated in the event of an area-wide disaster.
e. All data backups must be encrypted. In addition, backups must align to the retention, disposal, and destruction process. This includes establishing data protection control equivalency to the original data.
f. Backup and recovery processes and associated timelines should be reviewed at least annually to validate that defined recovery metrics and methods continue to meet business objectives.
g. Data backup and recovery processes must be tested on a periodic basis, at least twice per year, for a sampling of enterprise assets.

3.5 Communications

a. A disaster exists when so declared by an authorized person.
b. Recovery communication plans must be established and tested during business continuity and disaster recovery testing scenarios.
c. Recovery communications must include defined and scheduled communication mechanisms and relevant stakeholders. Preapproved and standardized communication templates should be created and used.
d. Public relations must be included in the BCP and DRP and include considerations for reputational repair and messaging to the public.

3.6 Testing, Maintaining, and Re-Assessing Business Continuity Plans

a. IOT and Entities should use a variety of testing techniques (e.g., tabletop exercises, live simulations) to provide assurance that the BCP will operate during an actual event.
b. The BCP and DRP should incorporate lessons learned from actual events and live scenarios.
c. The BCP and DRP should be reviewed annually and updated when changes to the environment warrant.

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.

P.09

Policy Name

Exceptions Management Policy

1. Purpose

The purpose of this Policy is to establish the process and conditions for accepting the risk created by noncompliance with the Statewide IT Policies and Standards. This Policy defines the requirements for tracking Exceptions through request, approval, continuous monitoring, and review. These requirements are designed to ensure compliance with all Statewide IT Policies and Standards unless there is an authorized business justification. This Policy also underscores the importance of proactive risk identification, planning for mitigation, and appropriate resource allocation for achieving mitigation.

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

An Entity may submit a written Exception Request to IOT. IOT will document the Exception in the State's Governance, Risk, and Compliance ("GRC") tool.

3.1 Request Management

a. The Requesting Entity must submit an Exception Request within the in the State's GRC tool.
b. Requests for Exceptions must follow the required fields within the GRC platform and be authorized by a designated State employee prior to submission. Further, the Request must document:
    i. The Policy or Standard for which the Exception is needed
    ii. The provision or sentence within the Policy or Standard for which the Exception is needed
    iii. The business justification and impact, including precise details
    iv. The identified risks
    v. The compensating controls that are planned or implemented to reduce the additional risks to a tolerable level
    vi. A remedial plan, including the planned deployment date for achieving remediation, whether remediation can be achieved with existing resources, and what additional resources would be required for achieving remediation
    vii. IOT may use information from Exception Requests to inform its enterprise Risk Register.
c. An Exception Request may address only a period of six months. If the noncompliance persists, the Entity must submit a new Exception Request with the updated information, including updates on the plan for remediation.
d. If the original Exception conditions have substantially changed, a new Exception Request must be submitted.

3.2 Acknowledgement

a. IOT must review Exception Requests. The Chief Information Security Officer or their appointed designee may acknowledge, deny, or seek additional information for Exception Requests.
b. All Exceptions must be reviewed.
c. Automatic renewal is not permitted.
d. If the remediation of an Exception is deployed, the Exception must remain in place until the solution or change is reviewed and fully implemented.

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.

P.10

Policy Name

Governance and Risk Management Policy

1. Purpose

The purpose of this Policy is to support information security governance and risk management for the State's network, data, and information systems. Information security risk management is the process of identifying and prioritizing threats to the 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

IOT will operate an information security risk management function to evaluate, monitor, and prioritize risks to the State's information systems.

3.1 Program Elements

a. IOT must implement procedures and guidelines for identifying, analyzing, and monitoring information security risks.
b. IOT must use framework-based measurements for assessing and quantifying information security risks and their potential impact to the organization.
c. IOT must have a process in place for risk acceptance, including consideration of Exception Requests.

3.2 Risk Identification

a. IOT must develop and implement a process for identifying and reviewing new and emerging information security risks. This process should use internal data, as well as external threat feeds where available.

b. IOT should conduct an annual review of information security risk.
c. IOT and Entities should notify the IOT GRC and Resiliency Services team of any new or emerging information security risks.

3.3 Risk Analysis and Prioritization

a. IOT should implement a best-practice method or tool for quantifying and measuring risk.
b. IOT and Entities should conduct risk assessments, especially of critical information systems.
c. Risk assessments may be conducted by IOT or a third party.

3.4 Risk Response and Treatment

a. IOT must have documented processes in place for responding to information security risks.
b. Entities should have documented processes in place for responding to information security risks.
c. IOT and Entities may respond to a risk by using one or more of the following methods:
    i. Avoid: Eliminate, withdraw from, or omit to engage in an activity creating risk
    ii. Transfer/Share: Transfer responsibility for the risk through processes such as, but not limited to, insurance
    iii. Reduce/Mitigate: Control the risk through additional or optimized controls
    iv. Accept: Accept the risk and plan for the expected impact

3.5 Monitoring and Management

a. IOT must collect and document mitigating activities associated with information security risks and establish a cadenced review.
b. IOT should produce a cybersecurity risk report quarterly, providing an update on information security risk trends, new or modified risks, and mitigation activity progress.

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.

P.11

Policy Name

Identity and Access Management Policy

1. Purpose

The purpose of this Policy is to establish the framework by which the State of Indiana manages the identity, authentication, and authorization of users and state information systems for ensuring the confidentiality, integrity, and availability of data and systems.

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 User Access and Account Management

a. An approved identity and access management ("IAM") platform must be used as the mechanism to manage resource permissions and the user account lifecycle.
b. IOT and Entities must assign a unique identifier for each user account, information asset, service, and workflow.
c. IOT and Entities will manage identity-management tools and centralized identity providers in a manner to prevent a user account from repudiating an action. This will include a cadenced review of user accounts.
d. User access activity must be logged and monitored to ensure the appropriate use of resources and to provide a record in the event of a malicious act.
e. Usernames and passwords will only be permitted and assigned to users who are authorized to use specific systems and domains.
f. IOT and Entities will use separation of duties in the creation and management of user accounts.
g. The State Personnel Department ("SPD") manages the authoritative source of truth for the identity of individuals employed by the State of Indiana. For other individuals working in the State Enterprise, IOT manages the authoritative source of truth for identity.
h. IOT must have identity-proofing processes in place. For further information, see the Access Management Standard.

3.2 Authentication and Password Requirements

a. IOT and Entities must use industry standard authentication methods, including multifactor authentication ("MFA"), where possible.
b. Failed authentication attempts must be limited to a defined number of total failed attempts and investigated by the appropriate team.
c. All authentication methods should be consistent with the determined authenticator assurance levels ("AAL"). This will include mandatory protections for preventing adversary-in-the-middle attacks, consistent privacy controls, and adherence to

requirements for record retention. Changes in assurance level may require reauthentication.

d. MFA tools must use approved authenticator options, such as software tokens, hardware tokens, and biometrics.
e. The use of short message service ("SMS") authentication is prohibited, unless other forms of authentication are not technically feasible.
f. Account passwords must follow industry standards and state guidance regarding password change frequency, complexity, and reuse. These requirements must align with the Password and Authentication Standard.
g. Users must be prompted for periodic reauthentication after session expiration or determined levels of inactivity.
h. IOT must manage an information system for authentication. That system should manage the creation, revision, and termination of credentials. IOT and Entities must integrate information systems:
    i. With the IOT-managed single sign-on ("SSO"), and
    ii. Using the technologies that IOT designates for this purpose.

IOT and Entities should authenticate pursuant to U.S. National Institute of Standards and Technology ("NIST") Special Publication 800-53. An Exception Request is required for any information system that does not authenticate through SSO.

3.3 Access Provisioning

a. User creation, access provisioning, and changes to access must be managed through a documented process. IOT and Entities are responsible for maintaining standard operating procedures related to management of the identity lifecycle.
b. A mechanism for submitting details on access changes, including purpose and business justification, must exist. This lifecycle must be tracked and documented in the appropriate ticketing system or identity platform.
c. Access entitlements should only be granted on a need-to-use basis and follow the principle of least privilege.
d. Role-based access control ("RBAC") guidelines should be in place so that individuals in specific roles have an allocated set of applications and access permissions based on role. An individual must have an assigned set of permissions consistent with role and job function.
e. IAM must include prompt changes in access when an individual changes roles.
f. Segregation of duties should be implemented to prevent users from performing inappropriate escalated functions.
g. Provisioning of additional levels of authorizations or new access requests must have proper management approval prior to provisioning.
h. Where applicable, Entities are responsible for managing the identity lifecycle and the associated authorizations of their users.
i. Remote access privileges must only be granted to individuals who meet defined requirements. Remote access must be secured and assigned in accordance with the Remote Access Policy.

3.4 Access Removal

a. Upon an individual leaving an Entity, transferring between Entities, or having a leave of absence greater than three months, IOT and an Entity shall deprovision and disable all the accounts related to that individual. This paragraph does not apply to SPD's authoritative source of truth for Identity.
b. IOT and Entity managers are responsible for submitting a formal notification to remove access from an individual who no longer requires access.
c. Access must be removed within 24 hours of an individual's termination.
d. A vendor, a prospective vendor, and any other seeking to do business with the State must review and comply with this policy. At IOT's written request, a third party must provide written assurance of compliance.

3.5 Access Review and Management

a. All requests regarding user IDs, passwords, and credentials should be communicated through approved support processes. IOT and Entity managers should perform a periodic review of workforce user access to determine if access is still required.
b. If a workforce manager identifies that an individual no longer requires access, the associated manager must complete the necessary paperwork as soon as possible to terminate access.

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.

P.12

Policy Name

Incident Response and Outage Response Policy

1. Purpose

The purpose of this Policy is to promote the effective and efficient response to cybersecurity incidents, privacy incidents, and outage events. This Policy also serves to implement Indiana Code Section 4-13.1-2-9.

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 Definitions

a. “Alert” and “Event” are synonymous and mean a report of suspicious activity, regardless of whether it is received from a person or an information system.
b. “Incident” means an Alert or Event that cannot be identified as an authorized action or process. “Incident” also means a failure that has the potential to impact an information system.
c. “Breach” means an Incident in which it is confirmed that a person or information system achieved unauthorized access to data or an information system.
d. “Loss” means a Breach that compromises the confidentiality, integrity, or availability of data or an information system.
e. “Outage” means an unplanned interruption to an information system or a reduction in the performance of the information system resulting from anything other than a person’s attempt to achieve Breach.
f. “Response” means an action taken to address an Incident, Breach, Loss, or Outage. Examples of a Response are sequestering a breached information asset, reimaging a breached information asset, and decommissioning a breached information asset.

3.2 Incident Response Plan

a. All Entities are encouraged to have an Incident Response Plan.
b. IOT must maintain and annually update an Incident Response Plan. IOT’s Incident Response Plan must include all of the following details:
c.
    i. Names, titles, and contact information for IOT staff responsible for the Incident Response Plan
    ii. Reference to playbooks, standard operating procedures, and other documents that address various types of Incidents, Breaches, and Losses
    iii. A communication plan for identifying, monitoring, investigating, and responding to an Incident, Breach, or Loss
    iv. Names of Entities’ primary reporters, secondary reporters, employees, contractors, and vendors responsible for incident response or who have been consulted in the course of an incident response
    v. Recommended means of contacting IOT Security, including for normal business hours and all other times
c. IOT must maintain information on Alerts, Events, Incidents, Breaches, and Losses that occur.
d. IOT must maintain a repository of cybersecurity incidents per Indiana Code § 4-13.1-2-2(a)(5).
e. IOT must maintain documented templates for formally assessing lessons learned following the activation of the plan or a training exercise.
f. IOT must annually train some of its personnel on its Incident Response Plan.
g. IOT must annually test its Incident Response Plan.
h. IOT must update its Incident Response Plan based upon testing and lessons learned in the course of its responsibilities.

3.3 Entity Responsibilities for Reporting and Notification

a. Pursuant to Indiana Code Section 4-13.1-2-9, an Entity must provide IOT with the name and contact information of the Entity’s employee who will act as its primary reporter.
b. The Entity may name others as secondary reporters. An Entity must update this information by September 1 of each year.
c. An Entity must notify IOT Security of an Incident, Breach, or Loss within eight hours of discovery.
d. An Entity must assist IOT in identifying, investigating, monitoring, and responding to an Incident, Breach, or Loss.

3.4 Interruption of Service

IOT and an Entity must communicate regarding whether to stop or restart the functioning of an information resource. Depending on the time sensitivity, likelihood, and potential severity of risk, IOT Security may stop the functioning of an information resource without receiving advance authority from the Entity. If this occurs, IOT Security must notify the Entity within one hour.

3.5 Outages

IOT and Entities should respond to an information system's loss of functionality resulting from anything other than a person's attempt to achieve a Breach. Please see the Outage Management 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.

P.13

Policy Name

Maintenance Policy

1. Purpose

The purpose of this Policy is to establish requirements for the logging, tracking, and managing of maintenance performed on the State Enterprise, including on-site and remote maintenance.

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 Operational Maintenance

a. IOT and Entities must specify the individuals authorized to perform maintenance.
b. A vendor to IOT or another Entity must submit to IOT a written description of its operational maintenance procedures within 30 calendar days of IOT's written request. This obligation applies regardless of whether the vendor's maintenance is performed by the vendor itself or a different organization.
c. IOT and Entities must establish procedures to ensure appropriate oversight of all maintenance activities on the systems they manage.
d. IOT and Entities must maintain the following maintenance records:
    i. Date and time the maintenance was performed
    ii. Names of staff performing maintenance
    iii. Name of the person who authorized the maintenance
    iv. Description of the maintenance performed
    v. List of replaced components
e. Any component removed from the system must be sanitized, pursuant to the U.S. National Institute of Standards and Technology ("NIST") Special Publication 800-53 Rev.5.
f. Maintenance tools must be inspected for malicious code as part of the authorization process. Approved tools must be documented. An individual performing maintenance must be trained on the tools available for use.
g. IOT and Entities must monitor maintenance activities and limit the time period in which maintenance may be performed.
h. Maintenance activities must follow IOT's change management process.
i. IOT and Entities must maintain warranties on servers. See the Asset Management Policy.

3.2 Entity Responsibilities

An Entity must establish and implement IT security procedures, including training, for the secure operation and maintenance of remote devices that fall outside of IOT's management.

a. Device operating systems must be maintained with appropriate vendor security patches and updates.
b. Mandatory system configurations, settings, and software for state-owned devices must not be modified without prior authorization by IOT.
c. Entities must develop guidelines on the management and maintenance of data.

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.

P.14

Policy Name

Physical Security Policy

1. Purpose

The purpose of this Policy is to establish the requirements for physical security of all systems, personnel, and information/media where IOT has people or assets.

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 Definitions

a. "IOT Space" means:
   A space, other than a residence, where an IOT employee, contractor, or consultant works,
   A space IOT uses for storage, and
   A space where IOT hosts the processing of data.
b. "IOT Individual" means an IOT employee, contractor, or consultant.
c. "Visitor" means anyone other than an IOT Individual. Visitors include vendors and employees of other state agencies.

3.2 Statement Regarding IOT Individuals

a. IOT must establish some control of public access to IOT Space.
b. IOT must provide an IOT Badge for authorized IOT Individuals.

c. An IOT Individual must wear his or her IOT Badge and keep it visible at all times while in IOT Space.
d. IOT managers are responsible for maintaining the accuracy of an IOT Individual's badge configuration by updating IOT Security regarding necessary changes.
e. IOT Security may manage the configuration of IOT Individuals' badge access. IOT Security needs at least 24 hours' notice to prepare appropriate badge configuration for an IOT Individual, regardless of whether it is the initial
a. configuration of badge access for that IOT Individual, a revision of that IOT Individual's badge access, or a termination of that IOT Individual's badge access.
f. IOT Security may issue a Temporary IOT Badge for no more than thirty calendar days.
g. In configuring an IOT Individual's access to physical areas, IOT will provide physical access to only those areas required for performance of the IOT Individual's duties.
h. An IOT Individual must notify IOT Security within an hour of discovering that his or her badge has been lost or stolen.
i. Tailgating is prohibited. An IOT Individual must present or scan his or her badge, as appropriate, regardless of whether a door or other means of ingress/egress is open.
j. IOT Individuals should report suspicious behavior to their manager. Managers are responsible for escalating any suspicious behavior.
k. IOT may use surveillance in IOT Space. There is no expectation of privacy in IOT Space.
l. IOT managers will review monthly: logs of physical access to IOT Space for purposes of identifying noncompliance with this Policy.
m. To the degree that an IOT Individual works out of another Entity's location, he or she must review, understand and comply with the respective Entity's policies and procedures.
n. An IOT Individual must lock a computer or mobile device when leaving it unattended in IOT Space.
o. On the last day of an IOT Individual's service to IOT, the IOT Individual's manager must meet with the IOT Individual to receive all physical tools assigned to the IOT Individual, including the IOT Badge, workstation, cell phone, tablet, headphones, and anything else they have been assigned. Also, the IOT Individual's manager must notify IOT's Identity and Access Management team to terminate the IOT Individual's physical and electronic access. The IOT Individual's manager must confirm that the IOT Individual's physical and electronic access was terminated.

3.3 Statement Regarding Visitors

a. IOT may provide a Visitor Badge for a Visitor upon sign-in.
b. A Visitor must wear and keep the Visitor Badge visible at all times. A Visitor must return the Visitor Badge when leaving the IOT Space. IOT will maintain a log of its providing and retrieving of Visitor Badges.
c. The Visitor Badge must be visibly different from the IOT Badge.
d. A Visitor may not enter or remain in an IOT Space without the presence of an IOT Individual. If a Visitor is observed to be without escort, an IOT Individual should escort the Visitor. Visitors must be escorted at all times.
e. IOT will not allow deliveries or service outside the normal business hours of the respective building unless an IOT manager has made a written confirmation of the delivery.
f. IOT may communicate other rules for Visitors.
g. This Policy does not apply to environmental services personnel.

3.4 Spaces of Increased Protection

a. IOT may adopt more stringent provisions regarding the physical security of data centers, disaster recovery sites, main distribution frames, intermediate distribution frames, and other physical areas of increased sensitivity.

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.

P.15

Policy Name

Remote Access Policy

1. Purpose

The purpose of this Policy is to promote the secure use of remote connections to the State network

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 Requirements for Remote Access

IOT and Entities must provide remote access as follows:

a. IOT must deploy tools for secure remote access to the State network, including multifactor authentication ("MFA").
b. Individuals must use IOT-provided tools, including MFA, to connect remotely to the State network. Individuals may only use a personal device if the device is authorized and registered in IOT's tool for mobile device management.

c. The User Policy applies regardless of whether the individual is connecting remotely. See the Acceptable Use Policy for more details.
d. All devices used to gain remote access, including desktop and laptop computers, smartphones, and tablets must be fully secured against common threats, and include updated antivirus software and all additional required security controls.
e. Remote access tools and platforms should be securely configured, including, but not limited to, access controls, system hardening, and the approved use of encryption when technically feasible.
f. Individuals with remote access privileges must only use their connection for work-related tasks and shall bear responsibility for any misuse.
g. IOT may disable unauthorized remote access tools.
h. IOT and Entities should conduct regular reviews of remote access tools and the individuals authorized to connect remotely.

3.2 Third-Party Remote Access

a. IOT may provide remote access to third-party vendors or business partners when there is a valid business justification.
b. Third-party individuals must comply with all requirements stated within the third-party agreement or within their contracted agreements with IOT or Entities.
c. Upon being granted access, third-party vendors must strictly adhere to this policy and all other related policies and standards.
d. Waivers, nondisclosure agreements ("NDA"), and other elements of official approval may be required prior to gaining remote access.

3.3 Wireless Network Considerations for Remote Individuals

a. An Individual may connect a state device to public Wi-Fi only if using an approved VPN client.
b. Individuals must follow IOT's standard for remote connection to the State network from their residence.

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.

P.16

Policy Name

Security Awareness and Training Policy

1. Purpose

The purpose of this Policy is to establish the requirements for a security awareness program.

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. Security Awareness and Training Administration

a. IOT must establish and maintain a security awareness program and provide training to Entities.
b. Users must complete any assigned security training.
c. IOT must establish and maintain a security awareness training platform to support hands-on phishing simulations. Phishing training should be of varying complexity to mirror current, active attack patterns.
d. The delivery mechanism will be through an online site or through the State's learning management system.

3.2 General Training and Awareness Requirements

a. The training is periodic in nature, as often as monthly. Users are required to complete assigned training within the specified time.
b. IOT will review and update the training content annually, or as needed, based upon the current, active threat patterns.
c. The following provides an example of a general set of items that are covered directly or indirectly as part of the overall training and awareness program:
    i. Email Security/Phishing
    ii. Information Protection
    iii. Passwords and Authentication Best Practices
    iv. Physical Security
    v. Social Engineering

3.3 Specialized and Role-Based Training

a. Entities should review opportunities to incorporate relevant role-based security training into their workforce (e.g., security-sensitive positions, executive leadership, privileged users, incident response).
b. Entities should train employees involved in managing sensitive data on data management and security practices related to

their specific roles. This is especially true regarding data protected by law and data received from a Federal agency, such as Protected Health Information ("PHI"), Federal Tax Information ("FTI"), and Criminal Justice Information Services ("CJIS") information.

c. IOT and Entities must use supplemental opportunities for enhancing security awareness through newsletters, awareness months, office visuals, and other communication mechanisms, where applicable.

3.4 Reporting and Remediation

a. Reporting will be provided to Agency management for completion rates, including specific users that have not completed a training.
b. Remediation training may be provided to users who fail specific training exercises, such as phishing simulations.
c. IOT may implement protective measures for a user that has not completed training.

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.

Policy Name

Security Operations Policy

1. Purpose

This Policy establishes the foundation for effective security operations, including the consistent logging of enterprise information systems, the compiling of log data, and the capacity to analyze and search the data for anomalous behavior and other indicators of threats.

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

IOT must deploy a security information and event management ("SIEM") tool for collecting, compiling, and analyzing State Enterprise log data it considers valuable for the functions identified in this Policy.

3.1. Threat Intelligence

a. IOT must maintain subscriptions to available threat intelligence services and have mechanisms in place for tracking internal and external sources of threat information.
b. IOT should have access to established sources of threat intelligence with a review process to confirm the efficacy of the sources.
c. Threat intelligence teams should share intelligence to provide for the improved detection of threats.
d. Threat intelligence teams should share indicators of compromise ("IOCs") to support security operations center ("SOC") analysts with their triage of alerts.

3.2. System Logging

a. Entities must configure systems to transmit security and audit logs to IOT's SIEM in accordance with the Security Logging Standard.
b. If an Entity maintains its own SIEM, it must configure systems to transmit security and audit logs to its own SIEM in accordance with the Security Logging Standard.
c. IOT should have a process in place to ensure that logging is enabled on information systems deemed critical.
d. IOT must have a standard time stamp for audit records, and a system that compares and synchronizes internal system clocks with an authoritative source for audit records.
e. Logging and monitoring systems must protect audit logging information and audit logging tools from unauthorized access, modification, and deletion in accordance with defined data protection and retention requirements.

3.3. Log Aggregation, Alerts, and Identification of Subjects for Incident Response

a. IOT must maintain the ability to review and search log data compiled from various information systems.
b. IOT and Entities must ensure adequate system capacity to meet data retention requirements.
c. IOT and Entities must establish business continuity and disaster recovery resources and processes for the continuity of threat intelligence.
d. Entities must notify IOT of federal, state, or other obligations regarding log retention.
e. IOT must establish a process for triaging alerts and identifying subjects for incident response.

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.

P.18

Policy Name

Security Tools Policy

1. Purpose

This Policy establishes the requirements for tools used to maintain and secure 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 Security Tool Requirements

a. IOT must select, maintain, and regularly review security tools.
b. IOT must deploy a standard set of security tools on end user devices and server infrastructure.
c. Endpoint detection tools must be broadly deployed across state assets.
d. Vulnerability management is as relevant with security tools as with any other information resource. See the Vulnerability Management Policy.

3.2 Endpoint Security Requirements

a. IOT will build and maintain systems from a standard configuration baseline, including cybersecurity hardening requirements.
b. For an endpoint device capable of running an antivirus software program, IOT and Entities must subscribe the endpoint device to the state antivirus service, with connectivity to support periodic virus signature file updates.
c. For an endpoint device capable of running a host-based threat detection and response software program, IOT and Entities must subscribe the endpoint device to the enterprise endpoint detection and response ("EDR") service, with connectivity to support periodic detection logic or rule updates.
d. Disabling or removing antivirus or EDR software, or disabling software updates to antivirus or EDR, is prohibited.

3.3 Application Security Requirements

a. Applications must be periodically scanned to identify application layer vulnerabilities. This includes dynamic scans of the functioning application, and static scans of the underlying source code and compiled binaries.
b. Vulnerabilities must be remediated according to defined timelines, based on the criticality.
c. Critical applications must be subscribed to the application security testing services, with connectivity to the central console to support periodic reporting.
d. Disabling application security testing services is prohibited.

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.

P.19

Policy Name

Software Development Policy

1. Purpose

The purpose of this Policy is to ensure security and due diligence in the development of software.

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. SDLC General Requirements and Environment

a. IOT and Entities that perform software development must establish and maintain a secure application development process ("software development life cycle" or "SDLC").
b. IOT must implement architecture designs, software development techniques, and system engineering principles that promote effective security within all information systems and assets. This should include referencing industry standards and leading practices.
c. IOT and Entities must protect data, pursuant to the Data Classification Policy and Standards.
d. IOT and Entities must logically separate development and testing environments from the production environment.
e. Separation of duties between development team members must be implemented, including the separation of roles between development personnel and those with the ability to push code into production.
f. Cybersecurity development techniques must be implemented following the SDLC to ensure that contractors, State-employed developers, and engineers are following the same unified process.
g. Developers should undergo specialized security training to enhance fundamental security skills.

3.2. Planning and Development

a. Roles must be identified to ensure that responsibilities for cybersecurity and privacy are established prior to development.
b. Security design principles, as well as privacy by design, should be established to ensure that relevant laws, regulations, and standards are considered during the software development process.
c. IOT may designate security requirements for the SDLC. In performing software development, individuals must consider industry standards and may incorporate threat modeling.
d. Common application vulnerabilities must be considered when planning development. Where possible, developers should use code-level security checks, such as static application security testing ("SAST"), to identify potential flaws.
e. Build and release pipelines must be managed by the assigned development teams.
f. Quality assurance testing must be performed by development teams to ensure that functionality is maintained and that all

security controls are in place.

g. Developers must not be granted local administrative access. Developers must work with system administrators to acquire software releases from manufacturers.

3.3. Validation and Monitoring

a. Vulnerability scanning is required on applications before being released into production.
b. Penetration testing may be required, depending on regulatory and application requirements and criticality.
c. IOT should define a systematic process to prioritize and triage identified security vulnerabilities, along with an acceptable level of risk for system releases. A release that exceeds a defined criticality may require an Exception.
d. Developers and engineers are responsible for root-cause analysis and correcting vulnerabilities.
    i. Vulnerabilities that have not been remediated must be tracked until they are closed.
    ii. Final testing of remediated vulnerabilities should be performed to validate that all issues have been resolved, and functionality is maintained.
e. Future maintenance must follow the SDLC to maintain security controls and prevent new vulnerabilities.
f. Post validation checks must follow the implementation process, where appropriate.

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.

P.20

Policy Name

Third-Party Risk Management Policy

1. Purpose

The purpose of this Policy is to establish requirements for third-party performance, accountability, and relationships with third parties.

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 Third-Party Risk Management

a. A "Third Party" means a vendor, service provider, contractor, consultant or any other organization considered for such status, with at least one of the following:
    i. Access to the State network, or
    ii. Impacts on the State network.
b. IOT and Entities are responsible for managing activities conducted by third parties, identifying and controlling the risks arising from such relationships, and ensuring that compliance with applicable regulations has been achieved.
c. IOT and Entities should assess, measure, monitor, and control risks associated with the use of a Third Party. This includes reputational, operational, financial, compliance, and cyber risks.
    i. Planning
        - IOT must maintain a Third-Party Risk Management Policy and Standard.
        - Entities are responsible for ensuring compliance with the policy and standard.
        - IOT and Entities must maintain an inventory of all third parties.
    ii. Due Diligence
        - IOT and Entities should perform due diligence to assess the risks associated with the potential use of a Third Party, including whether the Third Party is suspended, debarred, or otherwise excluded from contracting with the federal government or the State of Indiana.
        - After engaging a Third Party, IOT and Entities should perform cadenced reviews of the Third Party, its performance, the risks resulting from the relationship with the Third Party, and whether it has been suspended, debarred, or otherwise excluded from entering relationships with the federal government or the State of Indiana.
    iii. Contracting
        - IOT and Entities must define and use standard contract language in agreements with all third parties.
        - The standard contract language must include cybersecurity and IT requirements, and requirements for data management, at the conclusion of the relationship with the Third Party.

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.

P.21

Policy Name

Vulnerability and Patch Management Policy

1. Purpose

The purpose of this Policy is to establish the requirements for identifying and remediating vulnerabilities within the State Enterprise. This Policy also provides obligations for the Patching of tools and applications.

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 Identification and Discovery

a. IOT and Entities must implement and maintain a program to assess and track vulnerabilities on IT assets within the State Enterprise.
b. The vulnerability management program will incorporate the most currently available asset management data to refresh the

scope of Scans.

c. Regular penetration tests must be conducted to support the identification of potential vulnerabilities.
d. The program should also provide for a recurring feedback loop between vulnerability Scanning, Patch management, and configuration management processes to monitor for the remediation of identified vulnerabilities.
e. IOT must gather and analyze information on negative security events experienced by other organizations.
f. IOT may share information with Entities potentially impacted by identified vulnerabilities. At the discretion of the Chief Information Officer, IOT may share information on threats and vulnerabilities with external parties.

3.2 Vulnerability Scanning

a. IOT must use vulnerability-Scanning technologies ("Scan" or "Scanning") as a primary vulnerability management discovery mechanism.
b. IOT must Scan to identify the presence of vulnerabilities within operating systems, databases, some workstation applications, network resources, and other information resources owned or managed by IOT, such as cloud or Software-as-a-Service ("SaaS") applications.
c. IOT must Scan the following information resources at least monthly:
    i. All physical and virtual servers supported by IOT
    ii. All workstations supported by IOT
    iii. All network equipment supported by IOT
    iv. Internally developed applications (See the Development and SDLC Policy.)
    v. Commercial and proprietary cloud and SaaS application
d. An Entity or its vendor must Scan monthly to identify the presence of vulnerabilities within all applications that the Entity manages.
e. Entities, their employees, their contractors, and their vendors are prohibited from blocking the functionality of a Scanning technology.
f. Based upon information gathered through Scanning and information gathered on vulnerabilities exploited by other organizations, IOT and an Entity must determine whether to perform a remedial activity, the urgency for performing the remedial activity, and how to perform the remedial activity.

3.3 Patching

a. For an application managed by an Entity, the Entity must deploy a Patch ("Patch" or "Patching") provided by the manufacturer of the respective application. IOT must deploy other Patches.
b. Zero-day vulnerabilities with identified exploits must be prioritized and remediated within the required due date.
c. IOT may deploy a Patch without an Entity's prior authorization if the information resource is two or more Patches behind the manufacturer's most recently released Patch.
d. For all newly discovered vulnerabilities, Patch deployment should align with the chart below:

Severity Level	Severity Description	Remediation Service Level
Critical	Vulnerabilities with a CVSS score of 9.0 or higher and can be readily exploited or compromised with publicly available malware exploits.	Within 15 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps. Sooner if feasible.
High	Vulnerabilities with a CVSS score of 7.0 to 8.9 with no known publicly available malware exploit.	Within 30 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps.
Medium	Vulnerabilities with a CVSS score of 4.0 to 6.9 and can be mitigated within an extended time frame.	Within 90 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps.
Low	Vulnerabilities with a CVSS score of 0.0 to 3.9. Not all low-severity vulnerabilities can be easily mitigated due to application, operating system, and/or business requirements.	Within 120 days of identification and reporting, dependent upon the availability of a patch and/or remediation steps.

3.4 Validation, Testing, and Reporting

a. An Entity must test either (1) before deploying the Patch or other remediation within a non-production environment that is functionally identical to its production environment, or (2) after deploying the Patch or other remediation and at least eight hours before the next business day.
b. IOT must Scan information resources to determine whether a remedial activity was performed correctly. An Entity or its vendor must Scan an application to determine whether a remedial activity was performed correctly.
c. IOT will provide Entities with updated vulnerability metrics on a monthly basis.

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.

P.22

Policy Name

Standardized Enterprise Technology Policy

1. Purpose

The purpose of this Policy is to leverage common tools and efficiencies by standardizing the use of designated technologies throughout 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 Standard Technologies and Provisions

a. IOT must maintain a list of standardized technologies to be deployed throughout the State Enterprise, where possible. For certain relatively simple tools, there are benefits to having uniformity across the State Enterprise.
b. Please see Statewide IT Standards for provisions related to domain names, URLs, payment processors, and other subjects.

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.