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.