Indiana Office of Technology

Powering a State that Works

2024 Information Technology Resources User Policy and Agreement (ITR User Policy)

1. **Information Technology Resources** (IT Resources) includes all State-provided equipment, software, all types of confidential and sensitive data, and the State network. To use IT Resources, users must agree to abide by the terms of this policy. IOT may limit or revoke your ability to use IT Resources if you cease to abide by its terms.

2. **No Expectation of Privacy.** Users have no right to privacy related to their use of IT Resources. Any information created or stored on IT Resources is subject to public disclosure. The State reserves the right to monitor all use of IT Resources, including email, Internet history, and Internet traffic.

3. **User Requirements**

   A. **Protection of IT Resources.** Users must protect IT Resources from unauthorized access, theft, damage, and modification. The user must lock any computer screen by pressing Windows+L when not in use and protect State-provided equipment from theft and unauthorized use when outside the office.

   B. **Protection of State-Owned Data.** Users must protect all State-owned data and will not access or disclose information for which they have no authorization or business need.

   C. **Use of State-Provided Resources for State Business.** Only State-provided IT Resources are to be used for the business of State government, with exceptions authorized by agency policies and State ethics rules: Ethics Code. Users will not use State-provided equipment to conduct personal business or activities.

   D. **Use of Authorized Software**. Users must use only software included on the State Software Allow List or Enterprise Standard List in the Archer Software Portal.

   E. **Storage of Information.** Users must store State-owned data on State-provided storage media only. The storage of personal files on State-provided storage is prohibited.

   F. **Remote Access.** Users must connect to the State network through approved services only, including Citrix, VPN, and State-provided virtual desktop platforms. Personally owned computers and mobile devices may only be used for remote access if they are registered in the State mobile device management system.

   G. **Return of IT Resources at Separation.** Users are required to return IT Resources that have been provided to them by the State--computers, mobile phones, and all other devices--no later than at the time of their separation. Failure to return IT Resources will be viewed as theft and addressed accordingly.

   H. **Reporting Violations.** Users must report known or suspected violations of this agreement to the #ITR Violations email address.

   I. **Adherence to Security Guidelines.** Users must ensure that all security software remains enabled, including timely installation of updates on their State-provided devices, as directed by IOT.

4. **Prohibited Activities That Could Compromise the State's Security**

   A. **Unauthorized Users.** Users must not allow unauthorized users to access State-provided IT Resources or State-owned data.

   B. **Unauthorized Devices.** Devices used for State business must be approved by IOT. Users must not use personal or non-State-provided devices to access the State network without prior IOT approval.

   C. **Foreign Access.** Accessing State-owned data from foreign locations is prohibited. Agencies requiring or enabling employees to travel internationally must follow the International Travel Policy.

   D. **Unauthorized Posting to Social Media.** Users must not post to social media platforms from State-provided equipment unless essential to their job functions.

   E. **Disclosure of Login IDs and Passwords.** Users must not share login IDs or passwords to IT Resources with other people.

   F. **Personal Email Accounts.** Users must not use personal email accounts to conduct State business. Access to State IT Resources must be authorized.

   G. **Remote Control.** Users must not use remote-control software on internal or external systems unless approved by agency management and IOT.

   H. **Violation of Law.** Users must not use State-provided equipment to perform illegal or unethical activities, including violations of copyright or other intellectual property laws.

5. **Disciplinary Action.** Any inappropriate use of IT Resources or failure to comply with this agreement may result in disciplinary action, up to and including immediate dismissal from employment, criminal prosecution where the act constitutes a violation of law, and an action for breach of contract if applicable.

6. **Changes and Additional Information.** This policy will be updated annually; and users will agree to this agreement annually via the Success Factors learning module. This document and answers to frequently asked questions are located here: ITR User Policy. IOT Statewide Policies are located here: Statewide Policies in Archer.

7. **Acceptance Agreement & Acknowledgement.** Selecting **Agree** at the bottom of the module confirms your agreement to the terms and conditions pertaining to the ITR. Employees who decline to accept the terms and conditions must seek further guidance from their agency human resources office.