State of Indiana
Indiana Office of Technology

Information Resources Use Agreement (IRUA)

Information Resources are provided by the State to support the business of State government. The term "Information Resources" includes all State hardware, software, data, information, network, computing devices, phones, and other information technology. To use Information Resources, you agree to adhere to the provisions of this agreement which are established to ensure security and inform you of the conditions of use.

1. Appropriate Use.

a. Use for State Business. I understand that Information Resources are to be used primarily for the business of State government with exceptions limited to those provided by State Ethics Rules and my agency's policies.

b. Approved Information Resources. I shall only use Information Resources owned, licensed, or being evaluated by the State. I shall not use my personal Information Resources for State government business at State facilities (excludes personal cell phones and tablets when authorized by your agency). I shall not use Information Resources provided by a third party unless authorized by my agency.

c. Protecting from Misuse & Damage. I shall use care in protecting against unauthorized access, misuse, theft, damage, or unauthorized modification of Information Resources. I shall not leave a workstation without first ensuring it is properly secured from unauthorized access. I shall use good judgment to safely transport and store Information Resources in and away from the workplace.

d. Public Disclosure & Monitoring. I understand that any information created, accessed, or stored on Information Resources may be subject to public disclosure. The State reserves the right to monitor any and all use of Information Resources, including my e-mail and Internet use, and I have no right or expectation of privacy with respect to my use of Information Resources.

2. Prohibited Activities. I understand that activities prohibited by this agreement may not be permitted without the prior written approval of the CISO. Prohibited activities include:

a. Unauthorized Disclosure of Confidential Information. I shall not disclose confidential information to unauthorized parties. Confidential information includes but is not limited to social security numbers, driver's license numbers, financial account information, credit card numbers, and personal health information. I acknowledge that certain information is confidential or discretionary by law and it is my duty to protect that information from unauthorized disclosure.

b. Unauthorized Software. I shall not download or install any software outside of the State standards provided by my agency and IOT. Privately purchased or downloaded software without a legitimate State purpose or agency authorization is forbidden. Banned software includes, but is not limited to, sniffers, password crackers, games, screen savers, and peer to peer.

c. Violation of Law. I shall not use the Information Resources to violate any law, including copyright or other intellectual property law. I shall not copy, share or distribute software without authorization.

d. Unauthorized Use. I shall not permit unauthorized users to use the Information Resources that the State has provided me. I shall promptly report any unauthorized use to my manager or the CISO.

e. Access. I shall not share my password or access code to State Information Resources with any other person. I shall not use another person's password or access code. I shall not access or attempt to access information for which I have no authorization or business need. I shall connect to the State network only through approved services (e.g. – Citrix and VPN are approved; a direct dial-up connection to a work PC modem is prohibited).

f. Remote Control. I shall not use any remote control software or service on any internal or external host or systems not specifically approved by agency management, IOT support, and the CISO.

g. Circumvention of Security Measures. I shall not bypass or attempt to bypass measures in place to protect Information Resources from security threats and inappropriate use. I shall not disable software on computing devices designed to protect Information Resources.

h. Unauthorized Devices. I shall not place unauthorized computing or network devices on the State network (e.g. – computers, access points, etc.).

i. Unjustifiable Use of Resources. I shall not intentionally sustain high volume transactions or network traffic for non-business purposes. I shall not send or reply to messages that would negatively impact the performance of the email system (e.g. – "replying to all" on a message received in error). I shall refrain from actions that hinder others' use of Information Resources or that may increase State costs.

3. Storage of Information. I shall store State owned information only on State provided storage media. Storage of State information on non-State owned PCs, laptops, flash drives, CDs and other forms of media is prohibited. I shall not store State owned information resources on the Internet without express agency authorization. With appropriate authorization, I am allowed to access and store State email messages on my personal cell phone or tablet. The storage of personal or non-business music and video files on State provided storage is forbidden.

4. Adherence to Security Guidance. I shall ensure that security fixes and updates for my State provided resources are implemented consistently and promptly, as directed by IOT.

5. Spam/Phishing Awareness. I shall be aware of the characteristics of spam and phishing messages. I shall recognize and dispose of spam/phishing messages appropriately. I shall never provide my login ID and password as a result of an email or phone solicitation unless I'm completely certain it is from my agency or IOT. I shall not risk a malware infection by navigating to links embedded in spam messages.

6. Violations & Uncertainty. I shall report violations of this agreement to my manager or the CISO upon learning of such violations. If I am uncertain whether an activity is permissible, I will refrain from the activity and obtain authorization from my manager before proceeding.

7. Disciplinary Action. I am aware that any inappropriate use of Information Resources or my 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.

8. Changes and additional information. I understand this policy will be updated, the State will make reasonable efforts to inform me of the changes, and I am held accountable to abide by the current version posted at http://iot.in.gov/security/irua/. On this website I can also find IRUA clarifications and exceptions as well as answers to frequently asked questions.