



Effective: July 22, 2024

Page: 1 of 5

Cancels: New

POLICY-IS-4502

Approved by: Emily Bergkamp
Emily Bergkamp
General Manager

Heather Stafford Smith
Heather Stafford
Director, Administrative Services

Written by: Jason Aguero

INTERCITY TRANSIT TECHNOLOGY ACCEPTABLE USE POLICY

Definitions:

“Information Technology (IT) Assets/Resources” – Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

“Endpoint” - A computer or other device connected to a computer network. An endpoint may offer information resources, services and applications to users or other endpoints on the Network. Endpoints can include, but may not be limited to, desktop computers, laptop computers, network servers, portable computing devices (Android/iOS tablets and smartphones), embedded control systems and Internet of Things (IoT) devices. Also see: Mobile Device.

“Mobile Device” – Any hand-portable device capable of internet access, text, voice, email, instant messaging (IM), photo messaging or other types of data communication.

1. Individual accountability is required when accessing all [information technology \(IT\) assets](#) and organization information.
2. Agency information and [information technology \(IT\) assets](#) are the property of Intercity Transit and must be used in conformance with this policy, and applicable laws.
 - a. Agency IT assets are to be used to conduct Intercity Transit business. Personal use of Agency resources shall be in accordance with [Policy EX-0016 Use of Intercity Transit Resources](#) for additional information.

Effective: July 22, 2024

Page: 2 of 5

Cancels: New

POLICY-IS-4502

- b. Employees may not remove agency owned information and communications equipment from Intercity Transit premises or vehicles or modify Intercity owned vehicles or equipment without express permission from agency management.
- c. The following requirements apply to removable storage media, such as portable hard drives or flash drives:
 - i. Users may not copy agency data onto personal storage media.
 - ii. Unauthorized devices may not be plugged into agency assets.
- d. Minimal personal use of IT assets is permitted, provided such use is:
 - i. Consistent with Policy EX-0016 Use of Intercity Transit Resources
 - ii. Does not impede the ability of the individual or other users to fulfill the agency's responsibilities and duties, including but not limited to utilization of extensive bandwidth, resource, or storage.
 - iii. Does not compromise the security or integrity of agency technology/information assets.
 - iv. Agency may revoke or limit the personal use of agency resources privilege at any time.
- e. Users are prohibited from unauthorized changes of IT asset configuration.
- f. Users cannot connect personal devices to the agency corporate network without express permission from agency management.

3. Use of agency IT assets constitutes express consent for monitoring and/or inspection of:

- a. Any data users create, access, send, or receive.
- b. Any messages users send or receive.

Effective: July 22, 2024

Page: 3 of 5

Cancels: New

POLICY-IS-4502

- c. Any web sites that users access.

4. Intercepting, recording, or divulging private communication.

- a. Consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, that if the conversation is to be recorded that said announcement shall also be recorded.
- b. Pursuant RCW 9.73.030, all voice communications on agency communication systems shall be presumed recorded at all times. There shall be no expectation of privacy on all agency voice communication systems (includes radio, land lines, cellular and Voice over IP).

5. Access to systems does not guarantee personal privacy for any activity when using such systems. This includes legitimate agency purposes, minimal personal use, violations of acceptable use or any other use.

- a. Anyone authorized to access systems desiring privacy for de minimis personal use should not use agency IT assets. See section 4 of Policy EX-0016 Use of Intercity Transit Resources. See Policy FA-2512 Mobile Device for Agency Business for additional information regarding use of personal devices for official agency business.

Anyone using agency-issued [endpoints](#) is expected to exercise a reasonable level of protection over those devices.

- b. Endpoints must be used and stored in a manner to prevent unauthorized physical access.
- c. Users must physically secure unattended agency-issued endpoints from unauthorized access and must not leave the item unattended in publicly accessible areas.

6. Agency policies and contracts may restrict access to any websites, domains, or content.

- a. Anyone using agency IT assets to access the intranet, or the internet, must comply with all security policies to protect the confidentiality, integrity, and availability of agency information assets.

Effective: July 22, 2024

Page: 4 of 5

Cancels: New

POLICY-IS-4502

- b. The use of unauthorized software for content sharing is prohibited. Unauthorized connection of wireless access points, including cellular devices, to agency corporate networks is prohibited. Personal [mobile devices](#) may connect to the agency “guest” wireless network only.

7. Intercity Transit reserves the right to monitor agency-issued endpoints and computing devices.

- a. Agency-issued computing devices are assigned to users to assist them in the performance of their duties. The agency has the responsibility and right to monitor all aspects of agency IT assets.
- b. Information Systems must seize and work with employees to inspect any information asset and/or data stored on agency-issued endpoints during the investigation of a security incident or fraudulent activity.

8. Internet Use

The Internet will not be used to transmit information or knowingly connect to sites for an unlawful or prohibited purpose, including, but not limited to, the following examples:

- a. Discrimination on the basis of age, sex, marital status, sexual orientation, race, creed, color, national origin, citizenship or immigration status, honorably discharged veteran or military status, or the presence of any sensory, mental, or physical disability or the use of a trained dog guide or service animal by a person with a disability.
- b. Sexual harassment or sites containing sexual content
- c. Transmission of obscene materials
- d. Infringement on any copyright
- e. Expression of any campaign, political or religious beliefs
- f. The conduct of a personal, outside business, or other financial benefit or gain
- g. Unauthorized disclosure of protected health information

Effective: July 22, 2024

Page: 5 of 5

Cancels: New

POLICY-IS-4502

- h. Gambling
- i. Any form of discrimination or harassment

Agency management has the authority to monitor employee use of the agency Corporate and Guest networks.