Indiana Harbor Belt Railroad

Bring Your Own Device Policy

EFFECTIVE JANUARY 1, 2024

1. Overview

The need to establish proper guidelines for usage and control of Bring Your Own Devices (BYOD), as well as what they can access and what steps should be followed in the event of loss, theft, or employment termination is critical. Since employees use their devices for personal and/or recreational activities, this can pose more risk for the organization than the exclusive use of business-owned devices. This policy describes the steps that the IHBRR and its employees will follow when connecting personal computers and devices to IHBRR systems and networks.

2. Purpose

This policy outlines requirements for BYOD usage and establishes the steps that both users and the IT department should follow to initialize, support, and remove devices from company access. These requirements must be followed as documented to protect IHBRR systems and data from unauthorized access or misuse.

3. Scope

This policy covers all employees, contractors, consultants, temporary workers, and other personnel granted access to organizational systems, networks, software, and/or data.

4. Policy

The Equipment covered by this policy includes (but is not limited to):

- Desktops, laptops, and tablets
- Smartphones, iPod and similar personal devices that connect to Wi-Fi networks.
- Wearable devices such as watches, headsets, or any other Wi-Fi/Bluetooth enabled device.
- Personal gaming consoles (e.g., Xbox, PlayStation etc.) and handheld game devices are strictly prohibited from usage on The IHBRR network.

4.1 Policy Guidelines:

All users must understand that whenever a computer device is connected to the IHBRR's network, systems, or computers, opportunities exist for:

1. Introducing ransomware, viruses, spyware, or other malware.
2. Purposefully or inadvertently copying sensitive and/or proprietary IHBRR information to unauthorized devices.
3. Introducing a technical or network incompatibility to the organization that the user is not even aware of.
4. Loss of data may adversely affect the organization if it falls into the wrong hands.

As a result of any of these circumstances, a user connecting their own device to IHBRR resources, systems, or networks could interrupt business operations, cause unplanned downtime for multiple users, and/or cause a data breach releasing organization, client, and/or partner data to unauthorized parties. In worst-case scenarios civil and criminal penalties for the user and/or substantial costs and expenses to the organization could arise.

4.2 IT Department Responsibilities:

Where applicable, the IT department will ensure the following to facilitate BYOD access as requested for a user device:

1. Provide a copy of this document to any all employees, contractors, consultants, temporary workers, and other personnel that enact the use of BYOD.
2. The device does not have a static IP address that could introduce networking conflicts.
3. The device does not have a virus, spyware, or malware infection.
4. The device does not have any third-party software or applications that pose a threat to the systems and networks or that could introduce application incompatibilities (any such findings should be removed before proceeding).
5. The IT department reserves the right to make judgment calls regarding which applications (current or future) are appropriate for devices associated with or accessing IHBRR systems, networks, and data.
6. The device is properly protected against ransomware, viruses, spyware, and other malware infections and the system has properly licensed anti-malware software, when appropriate.
7. If this involves a mobile device that will be associated with IHBRR systems, a security policy may be applied to this device (such as via an Exchange server) to enforce a password/biometric/multi-factor authentication policy that will automatically lock the device after one-minute period of inactivity and erase the contents of memory and storage after a maximum of number failed authentication attempts.
8. This policy may also include the ability to remotely erase(wipe) these devices in the event of loss or theft.
9. The device has all critical and security patches installed.
10. The device is properly encrypted as necessary and applicable.
11. The device is properly configured to access resources remotely and that it does so in the most secure fashion possible, such as through a VPN connection or other approved encrypted communication software.
12. Appropriate screen and device locking mechanisms are in place.
13. When a device is to be decommissioned, the IT department will remove any required encryption, VPN, and anti-malware licensing from the user's device. It will also confirm that the user's device does not contain any traces of protected, sensitive, IHBRR, or proprietary information and will delete any that remains on the device.
14. IT will take appropriate measures to ensure that BYOD devices are not introduced into any system governed under the TSA Security Directive CIP, unless for a specified business need, and only after express approval by a member of senior management and/or IT management.

15. The IT department reserves the right (and should proceed) to remotely wipe a device if it has been lost or the employee has been terminated and has not brought their device to the IT department for decommissioning.

4.3 User Responsibilities:

1. Employees, contractors, consultants, partners, temporary workers, and other personnel should not connect BYOD devices to the IHBRR network without first consulting a member of IT for approval.
2. Employees, contractors, consultants, partners, temporary workers, and other personnel will take appropriate measures to ensure that BYOD devices are not introduced into any system governed under the TSA Security Directive CIP, unless for a specified business need, and only after express approval by a member of senior management and/or IT management.
3. The user should not attempt to change or disable any security settings applied to the device by the IT department.
4. The user should consult the manufacturer/vendor/carrier for support of their device before requesting assistance from the IT department.
5. If a user believes a personally owned or personally provided device that is authorized to connect to the IHBRR's resources, systems, or networks might be infected with a virus, spyware infection, or other malware threat or might be somehow compromised, they must immediately notify the IT department in writing of the potential security risk.
6. If a user loses or misplaces a personally owned or personally provided device that is authorized to connect to the organization's resources, systems, or networks, they must immediately notify the IT department in writing of the potential security risk.
7. Whenever a user decommissions, prepares to return, or otherwise ceases using a personally owned or personally provided device that the IT director has authorized for organization use, the user must notify the IT department that the device will no longer be used to connect to organization resources, systems, or networks.
8. Users may not discard previously authorized devices until the IT department approves the device for disposal.

5. Policy Compliance

5.1 Compliance Measurement

The IHBRR will periodically verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, automated scanning-monitoring etc.

5.2 Exceptions

Any exception to the policy must be approved by a member of IHBRR executive management in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- IHBRR_Acceptable_Use_Policy.docx
- IHBRR_Password_Policy.docx
- IHBRR_Workstation_Policy.docx
- IHBRR_Wireless_Policy.docx
- IHBRR_Remote_Access_Policy.docx
- TSA Security Directive Policy.docx

Andrew Feder
Andrew Feder (Dec 27, 2023 13:17 CST)

Dec 27, 2023

Andrew Feder, Senior Director of Information Technology

Date