Indiana Harbor Belt Railroad Company

Wireless Policy

EFFECTIVE JANUARY 1, 2024

1. Overview

There are an ever-increasing number of wireless devices such as cell phones, tablets, and laptops which utilize the IHBRR network. Insecure wireless configuration can provide an easy open door for malicious threat actors. A Wireless Access Policy will help mitigate risks to the IHBRR network.

2. Scope

All employees, contractors, consultants, partners, and temporary workers at the IHBRR, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the IHBRR must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the IHBRR network or reside on an IHBRR site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

The purpose of this policy is to secure and protect the information assets owned by the IHBRR. This policy specifies the conditions that wireless infrastructure end users and devices must satisfy to connect to the IHBRR network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the IHBRR Management team.

3. Policy

This policy provides a set of procedures and standards for usage of wireless technologies within the IHBRR network environment. The following rules and considerations apply with respect to usage of IHBRR wireless communications:

1. All wireless access points on the IHBRR network must be approved and centrally managed by the IT Operations team. Personal wireless routers (Netgear etc.) are strictly prohibited.
2. The addition of new wireless access points within IHBRR facilities will be managed at the sole discretion of IHBRR Management and IT Operations team. Non-approved installations of wireless equipment, or use of unauthorized wireless equipment on IHBRR premises, is strictly prohibited.
3. Due to bandwidth limitations, the wireless network should be viewed as a network to augment the wired network. Applications that require large amounts of bandwidth or are sensitive to changes in signal quality and strength may not be appropriate for wireless network use. Physical “ethernet” connectivity should be utilized for high bandwidth applications.
4. IT Operations may monitor wireless networks for performance, integrity, security and to ensure compliance with this policy.
5. IHBRR Management along with IT Operations reserves the right to deny any user or device access to the wireless network at any time.
6. Logical and physical user access to wireless network devices and services shall be restricted to authorized personnel and devices only.

7. Access to the IHBRR network must always follow IHBRR acceptable usage controls, authentication controls, and password policies.
8. Usage of the production wireless network is for the purpose of IHBRR business only. All other connectivity should be via the guest network.

4. Policy Compliance

4.1 Compliance Measurement

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

4.2 Exceptions

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

4.3 Non-Compliance

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

5. Related Standards, Policies and Processes

- IHBRR_Acceptable_Use_Policy.docx
- IHBRR_BYOD_Policy.docx
- IHBRR_Password_Policy.docx
- IHBRR_Workstation_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