Indiana Harbor Belt Railroad Company

Remote Access Policy

EFFECTIVE JANUARY 1, 2024

1. Overview

Remote access to the IHBRR network is essential to maintain our team's productivity, but in many cases remote access originates from networks that may at a significantly lower security posture than the IHBRR network. While these remote networks are beyond the control of the IHBRR, we must mitigate these external risks to the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to the IHBRR's network from any host at any location. These rules and requirements are designed to minimize the potential exposure to the IHBRR from damages which may result from unauthorized use of IHBRR network resources. Damages include the loss of sensitive or IHBRR confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred because of those losses.

3. Scope

This policy applies to all IHBRR employees, contractors, consultants, partners, temporary workers, and other personnel. This policy applies to IHBRR owned or personally owned computers, mobile computing devices, tablets, cell phones etc. used to connect to the IHBRR network. This policy applies to remote access connections used to do work on behalf of the IHBRR. This policy covers all technical implementations of remote access used to connect to IHBRR networks.

4. Policy

It is the responsibility of IHBRR employees, contractors, consultants, partners, temporary workers, and other personnel with remote access privileges to the IHBRR's network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

For additional information regarding the IHBRR's remote access connection options, including how to obtain a remote access login, troubleshooting, etc., contact a member of IHBRR Management or the IHBRR IT department.

The following policy rules apply with respect to IHBRR Remote Access:

1. Usage of unapproved VPN Client or Remote Access Software for access to the IHBRR network is strictly prohibited.
2. General access to the Internet for recreational use through the IHBRR network is strictly prohibited.

3. When accessing the IHBRR network from a personal computer, or other mobile device, Authorized Users are responsible for preventing access to any IHBRR computer resources or data by non-Authorized Users.
4. Performance of illegal activities through the IHBRR network by any user (Authorized or otherwise) is strictly prohibited.
5. Authorized users will not use the IHBRR networks to access the Internet for outside business interests.
6. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access
7. All hosts connected to IHBRR internal networks via remote access must be company-issued or approved third-party devices.
8. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs) and strong passphrases.
9. Users must exercise caution when connecting to networks in public venues like airports, coffee shops, hotels etc., and must not connect to the IHBRR's internal network (even via VPN) if on an unsecured, public network.
10. Authorized users shall always protect their login and password.
11. Access accounts used by remote vendors must only be enabled during the required period and must be disabled immediately thereafter. Vendor accounts must be closely monitored and approved by the IHBRR.
12. The sharing of remote access credentials with others is strictly prohibited.
13. Authorized Users shall ensure the remote host is not connected to any other network (other than the network used to establish remote connectivity) at the same time as remote connectivity to the IHBRR network.
14. Reconfiguration of a home user's equipment for the purpose of split tunneling or dual homing is not permitted at any time.
15. All hosts (personal workstations, tablets etc.) that are connected to IHBRR of Network internal networks via remote access technologies must use the up-to-date anti-virus software and/or malware protection enabled.
16. The copying of information, files, data etc. from the IHBRR network to a remote device (workstation, server, tablet, phone, other remote or cloud-based storage media etc.) is strictly prohibited unless otherwise approved by a senior member of IHBRR Management.
17. Users of Remote Access communications must report any suspicious activity (e.g., suspected phishing attack, malware attack, ransomware, unusual device behavior, etc.) to the IT Department and a member of senior management for the IHBRR immediately.

5. Policy Compliance

5.1 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.

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_BYOD_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