Indiana Harbor Belt Railroad Company

Acceptable Use Policy

EFFECTIVE JANUARY 1, 2024

1. Overview

The IHBRR has established this policy to assist in the protection of employees, contractors, consultants, partners, temporary workers, other personnel and the IHBRR itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Technology Information Systems, including but not limited to computer equipment, tablets, software, operating systems, storage media, network accounts providing email, web browsing, and FTP, are the property of IHBRR. These systems are to be used for IHBRR business purposes in serving the interests of the IHBRR, and of our employees, contractors, consultants, temporary workers, and other personnel during normal operations.

Effective security is a team effort involving the participation and support of every IHBRR employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer-network user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer-network equipment and operational technology systems at IHBRR. These rules are in place to protect the employee and IHBRR. Inappropriate use exposes the IHBRR to risks including virus attacks, ransomware, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices (including cell phones and tablets), and network resources to conduct IHBRR business or interact with internal networks and business systems, whether owned or leased by IHBRR, the employee, or a third party. All employees, contractors, consultants, partners, temporary workers, and other personnel at IHBRR are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with IHBRR policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to all employees, contractors, consultants, partners, and temporary workers, at the IHBRR, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by IHBRR.

4. Policy

4.1 General Use and Ownership

1. IHBRR proprietary information stored on electronic and computing devices whether owned or leased by IHBRR, the employee or a third party, remains the sole property of IHBRR. You must ensure through legal or technical means that proprietary information is protected in accordance with IHBRR policies, as well as state and local laws.
2. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of IHBRR data and proprietary information.
3. You may access, use, or share IHBRR proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of the Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
5. For security and network maintenance purposes, authorized individuals within the IHBRR may monitor equipment, systems, and network traffic at any time.
6. IHBRR reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. All mobile and computing devices that connect to the internal network must comply with all applicable IHBRR policies.

2. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3. Where possible, all computing devices must be secured with a password-protected screensaver. You must lock the screen or log off when the device is unattended.

4. Employees are not to post to newsgroups, blogs or social media from accounts with a IHBRR email address, unless otherwise approved by a member of IHBRR executive management.

5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware, phishing attempts, or ransomware. If in doubt of any content contact a member of IT so that they can review any suspected emails.

4.3 Unacceptable Use

The following activities are, in general, prohibited.

1. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

2. Under no circumstances is an employee, contractor, consultant, partner, temporary worker, and other personnel of IHBRR authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing IHBRR-owned resources.
3. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or IHBRR protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by IHBRR.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from digital web sources, magazines, books, or other copyrighted sources, copyrighted music or videos, and the installation of any copyrighted software for which IHBRR or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server, or an account for any purpose other than conducting IHBRR business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, ransomware etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using an IHBRR computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any IHBRR account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless performed by an approved member of the Information Technology team.

12. Executing any form of network monitoring which will expose, or intercept data not intended for the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network, or account.

14. Introducing network routers, wireless access points, network switches-hubs, or similar technology on the IHBRR network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, IHBRR employees to parties outside IHBRR, without strict authorization.

18. Usage of IHBRR computers, tablets or other devices for running a personal business or entertainment.

4.5 Email and Communication Activities

When using IHBRR resources to access and use the Internet, users must realize they represent the IHBRR. Whenever employees state an affiliation to the IHBRR, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the IHBRR". Questions may be addressed to the appropriate members of IHBRR executive management.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, phone, text, chat, blog, social media post etc.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within IHBRR's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by IHBRR or connected via IHBRR's network.

7. Posting the same or similar non-business-related messages to large numbers of blogging, group chat or social media sites.

4.6 Blogging and Social Media

Social Media and Blogging by employees, whether using IHBRR’s property and systems or personal computer systems, is subject to the terms and restrictions set forth in this Policy.

1. Social Media and Blogging from IHBRR’s systems are also subject to monitoring and blocking policies and procedures.

2. Employees shall not engage in any social media or Blogging posts that may harm or tarnish the image, reputation and/or goodwill of IHBRR and/or any of its employees.

3. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by IHBRR.

4. Employees may also not attribute personal statements, opinions, or beliefs to IHBRR when engaged in social media or blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of IHBRR. Questions may be addressed to the appropriate members of IHBRR executive management.

6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, IHBRR's trademarks, logos and any other IHBRR intellectual property may also not be used in connection with any social media or blogging activity unless expressly approved by a member of the IHBRR executive management team.

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_Wireless_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 13:18 CST)

Dec 27, 2023

Andrew Feder, Senior Director of Information Technology — Date