Indiana Harbor Belt Railroad Company

Password Policy

EFFECTIVE JANUARY 1, 2024

1. Overview

The IHBRR must develop, implement, and regularly review a formal documented process for appropriately creating, changing, and safeguarding passwords used to validate a user's identity and establish access to our information systems and data. All employees, contractors, consultants, partners, temporary workers, and other personnel with access to IHBRR information systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any IHBRR facilities, has access to the IHBRR network, or stores any non-public IHBRR information system assets.

4. Policy

4.1 Password Creation

1. Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.
2. User accounts that have system-level privileges granted through group memberships or programs such must have a unique password from all other accounts held by that user to access system-level privileges. Whenever possible, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.
3. All user-level and system-level passwords must conform to the Password Complexity Guidelines as outlined below:
    a) Passwords should not be based on something that can be easily guessed or obtained using personal information (e.g., names, favorite sports team, etc.).
    b) Passwords must have a minimum length of ten characters.
    c) Passwords must be composed of a mix of numeric, alphabetical, and special characters.
    d) Passwords should not be remembered or reused.

4.2 Password Change

1. Passwords should be changed at least every 180 days.
2. Password stress testing to include cracking or guessing may be performed on a periodic or random basis by the Information Technology team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to follow the

Password Complexity Guidelines.

4.3 Password Protection

1. Any user suspecting that his/her password may have been shared or compromised must report the incident and change all passwords.
2. Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential IHBRR information.
3. Passwords must not be communicated openly with an associated login in email messages.
4. Passwords should never be written (e.g., on a post-it note) and stored in an open or publicly accessible location.
5. Password lists should never be maintained in open text format.
6. Passwords may be stored only in "password managers" authorized by a member of Information Technology management team.
7. Do not use the "Remember Password" feature of applications (for example, web browsers).

4.4 Multi-Factor Authentication

1. Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

5. Policy Compliance

5.1 Compliance Measurement

The IHBRR will periodically verify compliance to this policy through various methods, including but not limited to, video/camera observation, 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_Workstation_Policy.docx
- IHBRR_Wireless_Policy.docx
- IHBRR_Remote_Access_Policy.docx
- IHBRR_BYOD_Policy.docx
- TSA Security Directive Policy.docx

Andrew Feder
Andrew Feder (Dec 27, 2023 13:16 CST)

Dec 27, 2023

Andrew Feder, Senior Director of Information Technology

Date