Belt Railway Company of Chicago Policies & Procedures

Policy No.: 1
POLICY: Information Technology Policy
POLICY VERSION: Version 1
Effective: January 1, 2022
Reviewed: November 29, 2021
Revised: December 2, 2021

I. Purpose

This policy outlines the following: (1) Acceptable Use of Information Technology Resources, (2) Password and Email Protocol, and (3) Network Access guidelines for the Belt Railway Company of Chicago (BRC). These rules are in place to protect both the employee(s) and the BRC. Inappropriate use of business technology exposes the BRC to risks including virus attacks, potential compromise of network systems and services, and legal issues.

All employees, contractors, consultants, temporary, and other workers are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with BRC policies and standards.

II. Policy Statement

BRC's electronic systems (including but not limited to the following: computers, phones, smart devices and all forms of Internet/intranet access) are to be utilized for authorized company business purposes. Brief and occasional personal use of the internet and email is acceptable if it is not excessive or inappropriate, occurs during personal time (lunch and/or other breaks), and does not result in an expense or harm to the company. BRC's electronic systems are the property of BRC, and any use of such systems is subject to review and monitoring by BRC. Employees, contractors, consultants, temporary and other workers have No expectation of privacy in their use of BRC's electronic systems.

III. Coverage & Distribution

This policy applies to the use of information, electronic and computing devices, and network resources utilized to conduct BRC business or interact with internal networks and business systems, whether owned or leased by the BRC, the employee, or a third party.

This policy will be provided to all employees, contractors, consultants, temporary, and others during initial Human Resources on-boarding/training process, and again as part of an annual policy review.

An acknowledgement document will be signed by all users of BRC IT resources. Supervisors must ensure that employees without internet access receive a printed copy of this policy and provide a signed acknowledgement form to Human Resources for records keeping purposes.

IV. Policy Overview

All users must:

- Store critical user/corporate data on network drives to facilitate backups
- Secure their technology and passwords
- Prevent theft of BRC equipment or data
- Complete any/all BRC required annual IT training
- Minimize non-work related Internet use (social media, personal finances and email)

Unless specifically authorized, all users must avoid:

- Releasing/exposing sensitive data (HIPAA, PTC/I-ETMS, corporate data)
- Excessive bandwidth usage (streaming video or music, file sharing)
- Risky computer use (unsecure email, Internet browsing, unsafe password use/release)
- Installing software or hardware without authorization from the IT Department (screensavers, utilities, USB drives, etc.)
- Illegal, unethical, and/or unsafe uses of technology (storing data insecurely, copyright infringement, threats, pornography, etc.)

V. Responsibilities for Compliance

Senior Director/Director of Information Technology – Define and enforce procedures. Conduct annual review and update the policy as needed.

All BRC employees, vendors and contractors – Review and sign the policy acknowledgement form and comply.

VI. Policy

(1) Acceptable Use of Information Technology Resources

General Use and Ownership:

BRC confidential information stored on electronic and computing devices (owned or leased by BRC, the employee or a third party) remains the sole property of BRC. Individuals have a responsibility to promptly report theft, loss or unauthorized disclosure of BRC proprietary information. Personnel may access, use, or share BRC proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

Business related use of streaming media is permitted if it does not negatively impact the corporate network or the user's job performance. BRC reserves the right to audit, limit or block access to streaming media. The BRC is not responsible for any information that the user views, reads, or downloads from the Internet.

Personal use of the computer system is considered acceptable, when the use is occasional, limited and does not:

- Interfere with the employee's work performance
- Interfere with any other user's work performance
- Negatively impact the BRC IT systems and/or network
- Violate any other provision of the BRC's policies, guidelines, or standards

Peer-to-Peer (P2P) file sharing/networking, that is not BRC business related is prohibited. Business related use of streaming media is permitted as long as it does not negatively impact the computer network or the user's job performance. BRC reserves the right to audit, limit or block access to streaming media. Avoid sending and/or downloading large files that could restrain the network.

Confidential data must never be sent via messaging technologies outside of the BRC approved corporate messaging systems. Financial and proprietary information is confidential and when disclosing this information, it must be in a secure format like an encrypted email. Personnel must not publish any information that is confidential and/or detrimental to the BRC on social networking sites.

Viruses, Trojans, Phishing and other malware can be easily delivered as an email attachment. Users should:

- Never open unexpected email attachments
- Never enter user id or email
- Never open email attachments from unknown sources
- Never click links within email messages, unless certain the link was sent intentionally (it is best to retype the link into your web browser)
- Immediately report any suspected or witnessed breach or message indicating a potential breach
- Never open non-work-related emails or spam
- Contact the BRC IT Department if you have concerns or questions

BRC Equipment and Software:
All technology purchases must be approved by the BRC IT Department, including, but not limited to, computers, tablets, phones, printers, etc. Exceptions to this policy can be granted by department managers. Software applications for BRC use must be approved by the IT Department.

Use of Personal Hardware, Software, and Email:

Users are prohibited from using third-party personal email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct BRC business. Non-company-provided computer equipment and storage devices are prohibited from being connected to the BRC network. Personal Smartphones are permitted on the BRC network, only if they are enrolled in the required Mobile Device Management "MDM" solutions established by the IT Department. The installation of non-company-supplied software applications is prohibited.

BRC reserves the right to monitor all use of BRC provided computer systems and networks.

(2) Password and Email Protocol
Password Construction:
Passwords must be at least eight characters in length. However, it is recommended that passwords be longer than 12 characters. If you choose a shorter password (less than 12 characters), passwords should contain the following: upper case letter, lower case letter, number, and symbol. A 2-factor authentication process maybe applied to some devices.

Passwords should not be constructed or contain the following:

- Sequential. i.e., W23 then W24 is not allowed. R22, j65 is allowed.
- A single word found in a dictionary (English or non-English)
- Birthdays and/or other personal information such as address and phone numbers
- Employee ID Number

- Word or number patterns like aaabbb, qwerty, zyxwdznuts, 123321, etc.

Password Protection Standards:

Do not use the same passwords for BRC accounts that are used for non-BRC accounts (e.g., personal Internet Service Provider accounts, option trading, benefits, G-Mail, Facebook, Amazon, etc.). Always use different passwords for various BRC access needs whenever possible.

Email:

BRC email accounts are to be utilized solely for business purposes. Email is an insecure method of communication, and information that is confidential, offensive, or unauthorized should never be sent in an email. Financial and proprietary information sent via email must be secured/encrypted. The BRC IT Department may implement internal controls to block excessive attachments and/or spam. Email signatures should be professional in nature.

(3) Network Access

Unsecure Networks:

Users are permitted to connect company-provided electronic devices to public or unsecured networks. Examples of unsecured networks include internet access from a home network, access provided by a hotel, an open or for-pay wireless hotspot, or any other network not under direct control of the BRC.

If BRC users are going to connect to unsecured networks, they must adhere to the following security guidance:

- When using a hotspot, log in or send personal information only to websites you know to be fully encrypted or contain a valid security certificate
- Do not stay permanently signed in to accounts, log out when your work is complete
- Do not use BRC passwords on non-BRC websites
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs - pay attention to these warnings
- Change the settings on your mobile device so it doesn't automatically connect to nearby Wi-Fi.
- BRC provides a secure VPN connection to encrypt traffic between your mobile device and BRC's network, even across unsecured networks. Organizations create VPNs to provide secure, remote access for their employees. VPN options are available for mobile devices; they can encrypt information you send through mobile apps.
- Check the URL of the sites you are on - look for “https” to help identify if it is secure

Remote Access:

It is the responsibility of BRC employees with remote access privileges to BRC's corporate network to ensure that their remote access connection is given the same consideration as an on-site connection. Performance of illegal activities via the BRC network by any user is prohibited. Users bear the responsibility and consequences of misuse.

Permanent third-party connections require that the link be held to higher security standards than an intra-company connection. Third-party user(s) must provide:

- Names and any other requested information requesting access (BRC reserves the right to approve or deny)
- 24/7 Contact information (email and phone) for the individual(s) responsible for the connection

VII. Enforcement & Violations

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor, vendor or other third party may result in the termination of the contract with the BRC.

If you have any questions regarding this document please contact your supervisor or the Human Resources Department.

VIII. Policy Definitions

Acceptable Use

Means that the device, internet or network use complies with BRC policies and procedures, including, but not limited to, those on harassment, copyright law, trade secrets, and confidentiality.

Bandwidth

The amount of information per unit of time that a transmission medium (like an internet connection) can handle.

Confidential Information

Confidential information is information which concerns or relates to the trade secrets, processes, operations, style of works, or apparatus, or to the production, sales, shipments, purchases, transfers, identification of customers, inventories, or amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or other organization, or other information of commercial value, the disclosure of which is likely to have the effect of either impairing the Corporation's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of the person, firm, partnership, corporation, or other organization from which the information was obtained, unless the Corporation is required by law to disclose such information.

NOTE: The term confidential business information includes "proprietary information”.

Data Leakage (Data Loss)

Data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems.

Data leakage may be malicious or inadvertent by users with good intentions.

Electronic Communications

Includes e-mail, instant messaging, social media and any other type of communication that is transmitted or received electronically.

E-Mail

Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.

Encryption

The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Encryption is used to protect data during transmission or while stored.

Excessive Use

Occurs if the usage interferes with normal job functions, responsiveness, or the ability to perform daily job activities.

Malware

Any software intentionally designed to cause damage to a computer, server, client, or computer network (by contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug).

A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware.

Messaging

A text or graphic-based application that allows two or more users to "chat" in real time.

Mobile Device

A portable device that can be used for certain applications and data storage. An example is a Smartphone.

Network Services

Network services are electronic resources that include, but are not limited to: e-mail, File Transfer Protocol (FTP), telnet, web browsing, and other Internet accessible services.

Password

A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Passwords are specifically managed thru the BRC Password Policy

Peer-to-Peer (P2P) File Sharing

A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Personal Use

The use of BRC devices, network or communications for non-work-related activity.

Phishing

A fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, instant messaging, and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Sensitive information

Information that is protected against unwarranted disclosure. Access to sensitive information should be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations.

Smartphone

A mobile telephone that offers additional applications, such as individual applications and email access.

Social Media

Any non-railroad website that allows the sharing of personal, professional or corporate information with peers or friends.

Spam

Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

Streaming Media

Information, typically audio or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

User

Any BRC employee or person who has been authorized to access BRC electronic information resources.

Belt Railway Company of Chicago Policies & Procedures

Policy No.: 1
Policy: Information Technology Policy Agreement
Policy Version: 1
Effective: January 1, 2022
Reviewed: November 30, 2021
Revised: December 2, 2021

I Agreement

I have received a copy, read and understand the Belt Railway Company of Chicago "BRC" Information Technology Policy.

I acknowledge and understand that BRC's network resources (hardware & software) are to be used for conducting company business. Personal use is permitted, but has limitations as outlined within the Information Technology Policy. I acknowledge that I have no right to privacy in connection with my use of BRC's network resources (hardware & software).

The BRC reserves the right to monitor and audit all company issued electronic communication systems and devices, access and review any or all records as needed, and retain and/or dispose of records as deemed necessary. Inappropriate or illegal use, or use which is detrimental to the interests of the BRC, its employees, customers or any other third parties, is strictly prohibited and may result in discipline, up to and including termination.

I understand that the policy applies to me while employed by the organization.

II Acknowledgement

_____ _____

Employee Signature Date

_____

Printed Name (First, Last)