Freightways

IT8 - PASSWORD POLICY

Purpose

The purpose of this policy is to set certain minimum requirements regarding password protocols and other authentication factors used in verifying a user's identity.

Policy Application

This policy applies to all members of Freightways group whether at a Freightways site or elsewhere and refers to all IT resources.

Definitions

Term	Definition
Critical data	Refers to the importance of the data to the operation of Freightways.
FIS	Freightways Information Services Limited
Freightways	Freightways Limited and its subsidiary companies together or individually as the context implies
Freightways Group	Includes all staff members (whether permanent, temporary or part time), contractors, subcontractors, consultants, business partners or official visitors or guests of members of **Freightways** staff.
Heads of unit	General Managers, Freightways CEO, Freightways CFO, Freightways CIO.
Information Security	The practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data.
MFA	Multi Factor Authentication a system that requires more than one distinct authentication factor for successful authentication. The three authentication factors are something you know, something you have, and something you are
Personal Information	Information about an identifiable individual
Sensitive data	Refers to data whose unauthorised disclosure may have serious adverse effect on individuals or on Freightways reputation, resources, or services
SaaS	Software as a Service.
Software	Includes all computer programs in machine readable and printed form, together with associated manuals and other related documentation.
Unit(s)	refers to an organisational grouping across **Freightways** and includes Business Units, Internal Service providers.

Key Relevant Documents

- Freightways – IT Security Policy
- NIST SP:800-63b

Roles and Responsibilities

Freightways group staff must maintain awareness and adherence to applicable IT policies, standards and guidelines. If you believe your password may have been compromised, please report the incident immediately to the FIS Service Desk and change your password.

IT has the right to reset passwords in the event of a suspected compromise of a user account.

Policy

1. For administrative and privileged access **MFA** must be enforced.
2. All administrative passwords must be at least sixteen [16] characters in length.
3. All application or service account passwords must be at least sixteen [16] characters in length and changed every 12 months unless compensatory controls exist to monitor account behavior, detect and remediate unusual activity.
4. All user passwords must be a minimum of ten [10] characters in length those between ten [10] and fifteen [15] characters will require the use of the following complexity and age requirements.
    a) Contain both upper and lowercase characters (a-z, A-Z);
    b) Contain both numeric and/or special characters (0-9, @#$%^&*() _+|~-=\` {} []:”; í <>? ./);
    c) Passwords must be changed every 12 months, unless compensatory controls exist to monitor account behavior, detect and remediate unusual activity.
5. Passwords of sixteen [16] characters or more shall not require any complexity or age requirements however, the use of passphrases or combination of multiple unrelated words to form a password is recommended (i.e. I drink c0ff33 all d4y)
6. Passwords must be completely unique, and not used for any other system, application, or personal account.
7. Passwords must not be a single dictionary word.
8. Default installation passwords must be changed immediately after installation is complete.
9. Application, personal account or systems should support passwords of up to sixty-four [64] characters long
10. Where possible, the checking of passwords against commonly used passwords and/or identified in data breaches lists should be completed.
11. For remote access systems the use of **MFA** must be enforced.
12. In the event you suspect your password has been compromised you must change your password immediately and notify IT.
13. Should IT become aware of a compromised account(s) they may force a password change immediately prior to user notification to protect sensitive or **critical data** and **personal information**.

Multi Factor Authentication (MFA)

Freightways group multifactor authentication requirement, at least two [2] factors of authentication must be used in combination of the following acceptable factors that can be used include:

- Password
- Mobile App Token (e.g. Forti token, Okta Verify, Microsoft Authenticator)
- Hardware Token (e.g. RSA or SAFENET fobs)
- Trusted Device (e.g. Okta Trusted or Azure Hybrid joined devices)
- Biometric (e.g. fingerprint or facial recognition)
- Location (e.g. Is the user connecting from their usual location)
- Electronic footprint (e.g. os client, browser version, time, location)

Password Protection

- Passwords shall not be written down or physically stored anywhere in the office. The use of a secure electronic password manager is encouraged.
- Passwords must not be shared with anyone, including IT. They should not be communicated via email, phone, or any technology.
- User IDs and passwords must not be stored in an unencrypted format.
- User IDs and passwords must not be scripted to enable automatic login. Service account IDs and password can be an exception to this requirement but must be managed in accordance with **unit** access management guidelines.
- “Remember Password” feature on websites and applications should not be used.
- All mobile devices that have access to or store **Freightways** data (e.g. Email) must be secured with a password and/or biometric authentication.