A black and white logo

Description automatically generated

**Metropolis Transit corporation**

**Password policy**

Contents

[Policy Statement 2](#_Toc149940437)

[password policy 2](#_Toc149940438)

[Owner of the policy 2](#_Toc149940439)

[External Resources Justifying the Policy 2](#_Toc149940440)

[Affirmative Procedure for Compliance 3](#_Toc149940441)

[Frequency of Compliance Audits 3](#_Toc149940442)

[Metric for Compliance 3](#_Toc149940443)

[Procedure for Collecting Compliance Metric 3](#_Toc149940444)

[Responsible Party(ies) for Updating the Policy 4](#_Toc149940445)

[Frequency of Policy Review 4](#_Toc149940446)

[Procedure for Updating the Policy 4](#_Toc149940447)

# **Policy Statement**

* set of **guidelines** and **rules** implemented by an organization to regulate and **secure** the use of **passwords by its employees and users**. It aims to ensure the **confidentiality**, **integrity**, and **availability** of **sensitive data** and systems by establishing best practices for creating, managing, and safeguarding passwords

## **password policy**

* The title "Password Security Policy **(P-123)**" signifies the specific focus of the policy on regulating the security aspects related to passwords within the organization.
* The inclusion of the identifier "**P-123**" serves to uniquely distinguish and manage the policy within the organization's broader documentation system.
* "Password Security Policy" clearly communicates the central theme of the document, highlighting its emphasis on **establishing** and **maintaining** **robust password practices**.

# **Owner of the policy**

* The Chief Information Security Officer (**CISO**) serves as the designated **owner of the Password Security Policy**, assuming the responsibility for overseeing its implementation, enforcement, and adherence within the organization.
* As the senior executive in **charge of information security**, the chief information security officer, or **CISO**, has the **necessary power and knowledge to decide on important matters** pertaining to the policy and how it will be implemented, making sure that it complements the organization's overarching security goals and plan.
* In the event of **policy updates** or **modifications**, the **CISO** is **responsible for orchestrating the necessary changes** and disseminating the **updated version** to all relevant departments, ensuring a consistent understanding and implementation of the revised guidelines.

# **External Resources Justifying the Policy**

* The Password Security Policy (P-123) is justified by compliance with industry regulations and emphasizes the importance of robust password practices to **safeguard sensitive data**.
* Requiring the use of **complex passwords** that include a combination of letters (both uppercase and lowercase), numbers, and special characters.
* Enforcing regular password updates, **prompting users to change their passwords** at predetermined intervals (e.g., every **90** days).
* Implementing **multi-factor authentication (MFA)** for an added layer of security, requiring users to provide additional forms of **verification**, such as a fingerprint scan or a one-time code sent to a registered device, in addition to their password.

# 

# **Affirmative Procedure for Compliance**

* Regular password updates are required to ensure that employees regularly change their passwords, **minimizing the risk of unauthorized access** due to compromised or outdated credentials.
* Prohibition **against sharing passwords** emphasizes the need for employees to maintain the confidentiality of their passwords**, reducing the risk of unauthorized** personnel gaining access to sensitive information.

# **Frequency of Compliance Audits**

* The Password Security Policy outlines **an annual audit frequency**, **ensuring that compliance with the policy's requirements** is thoroughly assessed and evaluated on a yearly basis.
* **Random spot checks are conducted quarterly**, allowing for intermittent assessments that serve as a proactive measure to monitor adherence to the policy's guidelines and identify any potential vulnerabilities or non-compliance issues in a timely manner.
* Audit results are carefully analyzed, and any identified areas **of non-compliance are promptly** addressed and remediated, reinforcing the organization's dedication to maintaining a secure and robust password management framework.

# Metric for Compliance

* The Compliance Metric for the Password Security Policy is based on **the percentage of employees who adhere to the specified password complexity guidelines**, ensuring that employees create passwords that meet the required standards for complexity and robustness.
* Regular monitoring and analysis of the **Compliance Metric facilitate the identification of trends and patterns**, allowing the organization to make informed decisions and implement necessary interventions to strengthen password security practices across the organization.

# **Procedure for Collecting Compliance Metric**

* The Metric Collection Procedure involves the regular conduction of password security **checks by the IT department**, which are designed to assess and **evaluate employees' adherence to the password security policy guidelines.**
* These checks are conducted at predetermined intervals, **ensuring that the organization maintains consistent oversight of its password security** practices and remains proactive in identifying any potential non-compliance issues.
* The analysis of the collected metrics enables the organization to identify **any patterns of non-compliance** or potential security **vulnerabilities**, facilitating the implementation of targeted corrective measures to address identified **weaknesses and enhance overall password security practices.**

# **Responsible Party(ies) for Updating the Policy**

* The Information Security Manager is designated as the **responsible party for overseeing updates to the Password Security Policy,** assuming the critical role of managing and maintaining the policy's relevance and effectiveness.
* The Information Security Manager **collaborates with cross-functional teams**, including IT professionals and relevant stakeholders, to **gather insights and feedback** that inform the policy update process, facilitating a comprehensive and holistic approach to policy enhancement.

# **Frequency of Policy Review**

* The frequency of the Password Security Policy review is a crucial aspect of maintaining an effective and **up-to-date security framework**. Here are some key points regarding the policy review frequency:
* Regular review intervals ensure that the Password Security **Policy remains relevant and aligned with the organization's evolving security needs** and industry best practices.
* The review frequency enables the identification of any outdated or inadequate security measures, **providing an opportunity to update the policy to reflect the latest security standards and regulatory requirements.**

# **Procedure for Updating the Policy**

* The Information Security Manager initiates the **updating** process **by gathering feedback** from relevant stakeholders and regulatory compliance teams, fostering a collaborative approach that incorporates diverse perspectives and expertise in **the review and revision of the Password Security Policy.**
* Based on the **insights and feedback gathered**, the policy undergoes comprehensive revisions to incorporate new **industry standards and address emerging security threats**, ensuring that the policy remains adaptive and resilient in the face of evolving cybersecurity challenges.