

Metropolis Transit Corporation.

Enterprise security policy.

Contents

[Policy Statement 2](#_Toc149868756)

[Owner Of the Policy 2](#_Toc149868757)

[Direction 2](#_Toc149868758)

[Scope 2](#_Toc149868759)

[Network Infrastructure: 2](#_Toc149868760)

[Data Handling 2](#_Toc149868761)

[Security Awareness 2](#_Toc149868762)

[Third-Party Relationships 2](#_Toc149868763)

[Legal and Regulatory Compliance 3](#_Toc149868764)

[Tone 3](#_Toc149868765)

[Roles And Responsibilities 3](#_Toc149868766)

[Information Security Officer (ISO) 3](#_Toc149868767)

[Information Technology team 3](#_Toc149868768)

[Human Resource team 3](#_Toc149868769)

[Information security team 3](#_Toc149868770)

[Management and security team 3](#_Toc149868771)

[Data Owners and End users 4](#_Toc149868772)

[Training Awareness and Security Programs 4](#_Toc149868773)

[Compliance 4](#_Toc149868774)

[Policy Review 4](#_Toc149868775)

[Data Classification 4](#_Toc149868776)

[Consequences of Non-Compliance 4](#_Toc149868777)

# Policy Statement

Metropolis Transit is committed to safeguarding its information assets and ensuring the confidentiality, integrity, and availability of data. This policy outlines the organization's information security framework to protect sensitive information and maintain regulatory compliance. It applies to all personnel, systems, and data associated with Metropolis Transit.

# Owner Of the Policy

The owner of the enterprise information security policy is typically the Information Security Officer (ISO). individual is responsible for overseeing all aspects of information security within the organization and ensuring that security policies, procedures, and practices align with the organization's goals and regulatory requirements.

# Direction

Metropolis Transit's information security direction should prioritize a proactive, holistic, and risk-based approach to safeguarding the organization's data and systems. The focus should be on prevention, detection, response, and recovery, all aimed at maintaining the confidentiality, integrity, and availability of critical information. It should also aim to align with industry best practices and regulatory requirements, addressing current and emerging threats.

# Scope

The scope of Metropolis Transit's information security strategy should encompass all aspects of the organization's operations.

## Network Infrastructure:

This includes the DMZ and router configuration for directing traffic into the four subnets, which is crucial for controlling the flow of data and ensuring secure access to various services.

## Data Handling

Information classification, encryption, and access controls should cover all sensitive data, whether in transit or at rest, in every part of the network.

## Security Awareness

Training and awareness initiatives should extend to all employees, contractors, and third parties who interact with Metropolis Transit's systems and data.

## Third-Party Relationships

Third-party security requirements should be applied to all vendors and service providers whose activities may affect the organization's security posture, such as: being involved with the security programs that are conducted as well as complying with the standards that the organization follows.

## Legal and Regulatory Compliance

Compliance should be maintained with relevant laws, regulations, and industry standards that pertain to Metropolis Transit's operations.

## Tone

The tone should emphasize the shared responsibility of all employees in maintaining a secure environment while fostering a culture of trust and collaboration.

# Roles And Responsibilities

## Information Security Officer (ISO)

The ISO is the overall owner of information security within Metropolis Transit. They are responsible for developing and implementing security policies, procedures, and controls. The ISO also oversees security training and awareness programs and ensures compliance with security regulations and standards.

## Information Technology team

* ensuring that data transmitted by IoT devices is encrypted to protect sensitive information. They should implement encryption methods and key management practices.
* In collaboration with the Network Security team, is responsible for configuring and managing the firewall to control incoming and outgoing network traffic. They should regularly review and update firewall rules to ensure they align with the organization's security policy.
* implement and maintain intrusion detection and prevention systems. They must monitor the network for unusual activities and respond to potential security threats.

## Human Resource team

Mainly they are responsible for Enforcement and Consequences by working beside the ISO to enforce security policies and address violations They should establish clear consequences for policy violations and ensure consistent enforcement. As well as providing security awareness and training programs.

## Information security team

* responsible for developing and maintaining an incident response plan. They must define procedures for identifying, reporting, and responding to security incidents, and they should oversee incident containment and recovery efforts.

## Management and security team

Mainly, they are responsible for physical security by ensuring data centers, equipment, and facilities are protected with access controls, surveillance, and environmental controls.

## Data Owners and End users

Data owners are responsible for classifying and protecting data under their control, in accordance with this policy, All employees are responsible for adhering to security guidelines, reporting security incidents, and participating in security awareness and training programs.

# Training Awareness and Security Programs

[Security Awareness Program Timeline.docx](Security%20Awareness%20Program%20Timeline.docx)

# Compliance

All users, including third parties, shall comply with Policies to comply with ISO standard that the company aims to obtain , and any noncompliance or misuse may result in a formal disciplinary action based on the Human Resources disciplinary process, and the compliance is audited once each three years.

The Compliances is achieved by creating an affirmative procedure:

Policy Review:

Ensure that you have read and understood the organization's Information Security Policy. If you have questions or require clarification, contact the Information Security Officer (ISO), and ensure on continuous update on the policy each year.

Data Classification:

Understand the classification of data you work with. Identify whether the data you handle is sensitive, confidential, or public.

* Sensitive Information: Includes proprietary data, personally identifiable information (PII), and confidential business data.
* Personal information
* Confidential Information: Information that, if disclosed, could harm the organization or its customers.
* Public Information: Non-sensitive information intended for public consumption.

## Consequences of Non-Compliance

Understand that non-compliance with the policy may result in disciplinary actions, including warnings, suspension, or termination, depending on the severity of the violation.