A black and white logo

Description automatically generated

Metropolis Transit corporation

Operation management policy

Contents

[**Policy Statement** 2](#_Toc149931680)

[Operational Procedures and Responsibilities. 2](#_Toc149931681)

[Control of Operational Software. 2](#_Toc149931682)

[Malware Protection. 2](#_Toc149931683)

[Logs Protection. 3](#_Toc149931684)

[Clock Synchronization. 3](#_Toc149931685)

[Patch Management. 3](#_Toc149931686)

[Technical Vulnerability Management and Penetration Testing. 3](#_Toc149931687)

[Information Backup. 4](#_Toc149931688)

[**Owner of the policy** 4](#_Toc149931689)

[**Compliance** 5](#_Toc149931690)

[Procedure 5](#_Toc149931691)

[Measurement 5](#_Toc149931692)

[**Update and Review the policy** 5](#_Toc149931693)

# **Policy Statement**

## Operational Procedures and Responsibilities.

* 1. Metropolis company shall develop and prepare appropriate documented operational procedures for system activities associated with information technology and communication facilities such as:
     1. Installation and configuration of systems.
     2. Backup and Restoration.
     3. Monitoring procedures.
     4. Media Handling.

## **Control of Operational Software.**

* 1. Procedures shall be implemented to control the installation and updating of software on operational systems.
  2. Users shall be prohibited from installing and downloading unauthorized software, only the approved whitelist software by IT Department shall be installed.
  3. IT Department shall maintain and update application whitelisted.
  4. Administrators shall ensure that Information Security controls in place, are effective, and are not being bypassed. Such controls shall include, but not limited to:
     1. Patching systems regularly.
     2. Following change management process before implementing any change.
     3. Following access management process before granting any access, immediately revoking access for leavers, and immediately modifying access for transferred user

## Malware Protection.

* 1. Metropolis shall have well-defined mechanism to prevent and detect viruses and malicious software and recover infected systems in a proper and timely manner, through a combination of user education and appropriate anti-virus technology.
  2. company shall prevent the use of unauthorized and unlicensed software and utilities on its computer systems.
  3. Anti-virus software shall be updated on all devices on a frequent basis. The frequency of this update shall be at least once daily.
  4. The anti-virus logs shall be backed up and shall be available for any investigation requirements in case of virus malicious software attack incidents.

## 

## Logs Protection.

* 1. Logs and SIEM solution shall be protected against tampering and unauthorized access.
  2. Controls shall aim to protect against unauthorized changes and access to logs, including:
     1. Activity logs that are being edited or deleted.
     2. Encrypting the logs.
  3. Controls shall also aim to protect the availability of the logs, by:
     1. Having a copy of the logs in the storage.
     2. Logs shall be backed up, as per the “Backup Policy”.
     3. Retention period for Information Security event logs shall be at least 12 months, first 3 months available on-line.

## Clock Synchronization.

* 1. The clocks of all relevant information assets within company shall be synchronized to an accurate and trusted reference time source.
  2. The company shall use the Network Time Protocol (NTP) to keep all the servers in synchronization with the master clock.

## Patch Management.

* 1. Patch management scope shall include at least network devices such as the router R1 and R2, client devices and peripherals (e.g., desktop, laptop, tablet computers, smartphones, and printers).
  2. All hardware, operating systems, database, applications, enterprise applications, firmware, and middleware.
  3. Software, applications, and devices shall be patched at least:
     1. On a monthly basis for external systems and for systems that can be accessed through internet.

## Technical Vulnerability Management and Penetration Testing.

* 1. Technical vulnerabilities shall be identified in a timely fashion, evaluated and appropriate measures taken to address them.
  2. Technical vulnerabilities shall be classified based on their criticality level.
  3. Source code review on the annual basis.

## Information Backup.

* 1. Backup copies of information, software and system images shall be taken and tested regularly.
  2. All critical applications and information for critical business processes shall be backed up.
  3. Backup copies of critical applications and information for critical business processes shall be maintained and tested regularly to support Disaster Recovery and Business Continuity.
  4. Media backups for business-critical systems shall be stored in a secure off-site location.

# **Owner of the policy**

These policies are essential for the proper functioning and security of an organization's IT infrastructure, and as such, they are typically under the purview of the IT leadership, in which they are mainly responsible for:

* 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.

The Chief Information Officer (CIO) or the Director of IT Operations is often responsible for developing and overseeing operational management policies, including those related to Control of Operational Software, Malware Protection, Logs Protection, Clock Synchronization, Patch Management, Technical Vulnerability Management, Penetration Testing, and Information Backup.

# **Compliance**

## Procedure

In the operational management policy, provide a clear set of guidelines and procedures that employees and relevant stakeholders must follow to be compliant with the policy. It could involve instructions for installing security software, configuring logging, and maintaining software patches. Training and awareness programs for employees can be included as part of compliance procedures. Which is audited annually.

## Measurement

Define the key performance indicators (KPIs) or metrics that will be used to measure compliance with each aspect of the policy.

* Malware Protection: Frequency of malware scans and percentage of devices with up-to-date antivirus definitions.
* Logs Protection: Percentage of log files that are protected from unauthorized access.
* Clock Synchronization: Accuracy of clock synchronization within the organization.
* Patch Management: Percentage of systems with up-to-date patches.
* Information Backup: Success rate of data backups and recovery procedures.

# **Update and Review the policy**

Specify who is responsible for maintaining and updating the Operation management policy which is the IT team and the review for updates is conducted annually or whenever change occur in the organization or the regulations and standards that the organization want to comply with.

If there is a need to update that should follow a specific procedure:

1. Initiation of Updates:

Anyone within the organization can propose updates to the operational management policy. This could be based on changes in technology, regulatory requirements, security threats, or feedback from employees or stakeholders.

1. Review Proposal:

A review committee or designated individuals responsible for policy updates should evaluate the proposed changes. This review committee may include representatives from IT, IT security, compliance, and other relevant departments.

1. Impact Assessment:

Assess the potential impact of the proposed changes on the organization, including its operational procedures and responsibilities. Consider the benefits, risks, and resource implications of the updates.

1. Drafting Updates:

If the proposed changes are approved during the review, draft the updated sections of the policy. Ensure that the language is clear, specific, and aligned with the organization's goals and regulatory requirements.

1. Approval Process:

Clarify the approval process, including the individuals or roles responsible for granting final approval. This could be the CIO, CISO, or other relevant executive roles. All proposed changes should be reviewed and approved before implementation.

1. Documentation and Communication:

Maintain comprehensive documentation throughout the update process. This documentation should include records of discussions, decisions, impact assessments, and approvals, communicate the changes to all relevant stakeholders. This could involve distributing the revised policy, conducting training sessions, or providing awareness campaigns to ensure that employees understand the changes.

1. Implementation:

Implement the approved changes in line with the policy updates. Ensure that all operational procedures and responsibilities are aligned with the updated policy.

1. Monitoring and Auditing:

Establish monitoring and auditing procedures to ensure that the updated policy is effectively implemented and that compliance is maintained. Regularly review and assess compliance with the new policy.

1. Feedback Mechanism:

Provide a mechanism for employees and stakeholders to provide feedback on the updated policy. This feedback can be valuable for ongoing improvement and ensuring that the policy remains effective.

1. Review Schedule:

Specify how often the updated policy will be reviewed for further updates. This could be done annually or at other intervals as necessary, and track changes to the policy over time.