A black and white logo

Description automatically generated

Metropolis Transit corporation

Information Security Risk Management Policy

Contents

[Policy Statement 2](#_Toc149936984)

[Information Security Risk Management Policy 2](#_Toc149936985)

[Owner of the policy 2](#_Toc149936986)

[External Resources Justifying the Policy 2](#_Toc149936987)

[Affirmative Procedure for Compliance 3](#_Toc149936988)

[Frequency of Compliance Audits 3](#_Toc149936989)

[Metric for Compliance 3](#_Toc149936990)

[Procedure for Collecting Compliance Metric 4](#_Toc149936991)

[Responsible Party(ies) for Updating the Policy 4](#_Toc149936992)

[Frequency of Policy Review 4](#_Toc149936993)

[Procedure for Updating the Policy 5](#_Toc149936994)

# **Policy Statement**

* the significance of safeguarding critical data, systems, and networks from potential threats and vulnerabilities.

## **Information Security Risk Management Policy**

* By emphasizing "risk management" in the policy title, the organization demonstrates a proactive stance in identifying**, evaluating, and mitigating security risks**. This **highlights the organization's dedication to ongoing assessment and management** of the dynamic security landscape, showcasing a strategic and comprehensive approach. The focus on risk management promotes a culture of vigilance and preparedness, encouraging a collective commitment to addressing potential security threats effectively within the organization.

# **Owner of the policy**

* Chief Information Security Officer **(CISO)**
* The CISO's responsibilities extend beyond mere policy enforcement; they are also entrusted with the **critical task of ensuring that the organization's security posture remains robust and adaptive to the constantly evolving threat landscape.** Their seniority within the organizational hierarchy grants them the authority necessary to allocate resources, implement security protocols, and enforce compliance across all departments effectively. Moreover, the CISO's direct access to the executive leadership team facilitates seamless communication and alignment of security objectives with the organization's overarching strategic goals and vision.

# **External Resources Justifying the Policy**

* ISO 27001 is an internationally recognized standard for Information Security Management Systems (ISMS), emphasizing a systematic approach to managing **sensitive information**.
* Compliance with ISO 27001 demonstrates the organization's commitment to maintaining the **confidentiality**, **integrity**, and **availability** of data through comprehensive risk assessment and security control implementation.
* GDPR (General Data Protection Regulation) is a stringent data protection regulation that emphasizes the protection of personal data and privacy rights for individuals **within the European Union and the European Economic Area**.

# **Affirmative Procedure for Compliance**

* Mandatory **annual** security **awareness training** ensures that employees understand their roles in **maintaining** the organization's security posture.
* Security awareness training equips employees with the **knowledge** and **skills** necessary to **recognize** and **respond** to various security threats, minimizing the likelihood of successful security breaches resulting from human error or negligence.
* Conducting vulnerability assessments at defined intervals allows the organization to **proactively detect and address any existing or emerging vulnerabilities**, reducing the likelihood of exploitation by malicious actors.

# **Frequency of Compliance Audits**

* **Annual** audits are scheduled to ensure a **regular and systematic review** of the organization's adherence to the Information Security Risk Management Policy.
* Conducting audits annually allows for a **comprehensive evaluation of the organization's overall security** posture and the effectiveness of security controls.
* The choice of annual **audits reflects the organization's commitment to maintaining a robust and effective information security framework**, fostering continuous improvement and resilience against potential security risks.

# Metric for Compliance

* Tracking the **percentage of completed security awareness training** provides a quantitative measure of the organization's efforts to **educate and empower employees** in understanding and adhering to security protocols and best practices.
* Analyzing the percentage of completed security awareness training helps in identifying **any gaps or areas where additional training or resources may** be **needed**, facilitating targeted improvements in the overall security awareness program.
* Analyzing these metrics over time facilitates the **identification of trends and patterns**, allowing the organization to continuously refine its security awareness program and **vulnerability management** processes to adapt to evolving security challenges and emerging threat landscapes.

# **Procedure for Collecting Compliance Metric**

* Delegating the responsibility of metric collection to the Human Resources (**HR**) and Information Technology (**IT**) departments **ensures the accurate and efficient recording of data** related to security awareness training and vulnerability management efforts.
* Entrusting the **IT department with the responsibility of recording** and **tracking** **vulnerabilities** allows for the **systematic documentation** of identified security weaknesses, their prioritization, and the implementation of remediation measures.
* The **collaboration** between the **HR** and **IT** departments in metric collection facilitates the integration of data from multiple sources, **providing a comprehensive and holistic view** of the organization's security awareness and vulnerability management efforts.

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

* Involving the Chief Information Security Officer (**CISO**) and Chief Technology Officer (**CTO**) in policy updates leverages their specialized technical expertise and industry knowledge, **ensuring** that the **policy remains current and effective in addressing the organization's evolving security needs.**
* The **CISO's** in-depth **understanding of cybersecurity** best practices and the **CTO's knowledge of technological** advancements enables the policy to align with the latest security trends, emerging technologies, and industry-specific regulatory requirements.
* The active participation of the **CISO** and **CTO** in policy updates demonstrates the organization's commitment to maintaining a proactive and strategic approach to information security, **safeguarding** the organization's **assets** and **data** against evolving **cybersecurity** **threats** and challenges.

# **Frequency of Policy Review**

* Conducting **bi-annual** policy reviews **ensures that the policy remains current and adaptable to the rapidly** evolving information security landscape, enabling the organization to stay abreast of emerging security trends and best practices without overwhelming the operational workflow.
* Regular policy reviews enable the organization to **respond promptly to changes in the regulatory environment and industry standards**, ensuring that the policy **remains compliant** with the latest legal requirements and security regulations.

# **Procedure for Updating the Policy**

* Conducting a comprehensive review of the policy **during updates** involves a thorough **examination of the policy's effectiveness**, relevance, and alignment with current security trends and regulatory requirements.
* Communication of policy **changes to relevant stakeholders** ensures that **all employees and concerned parties are informed** about any modifications, facilitating a clear understanding of the updated policy guidelines and expectations.