A black and white logo

Description automatically generated

Metropolis Transit corporation

information security awareness and training policy

Contents

[Policy Statement 2](#_Toc149929117)

[SECURITY AWARENESS TRAINING 2](#_Toc149929118)

[Owner of the policy 2](#_Toc149929119)

[External Resources Justifying the Policy 3](#_Toc149929120)

[Affirmative Procedure for Compliance 3](#_Toc149929121)

[Frequency of Compliance Audits 3](#_Toc149929122)

[Specific Metric for Measuring Compliance 4](#_Toc149929123)

[Procedure for Collecting Compliance Metric 4](#_Toc149929124)

[Responsible Party(ies) for Updating the Policy 4](#_Toc149929125)

[Frequency of Policy Review 5](#_Toc149929126)

[Procedure for Updating the Policy 6](#_Toc149929127)

# **Policy Statement**

* + to guarantee that every Information Technology (IT) user receives the proper degree of information security awareness training.
  + This policy is applicable to all departments and users of IT resources and assets.

## **SECURITY AWARENESS TRAINING**

* Include security awareness instruction in the first training that new users receive.
* Arrange security awareness training when information system modifications necessitate it.
* Based on the unique organizational requirements and the information systems to which personnel has authorized access, IT shall decide the appropriate content of security awareness training and security awareness techniques, The content shall:
* Contain a fundamental comprehension of the necessity of information security as well as user actions to preserve security and react to alleged security incidents.
* Talk about the importance of operations security awareness. Displaying posters, providing materials with security reminders, creating email advisories or notices from senior organizational officials, putting messages on the login screen, and holding information security awareness events are a few examples of security awareness strategies.

# **Owner of the policy**

* Chief Information Security Officer **(CISO)**
  + **The information security awareness and training policy owner** is responsible for **working closely** with **human resources**, department heads, and other stakeholders to effectively communicate and enforce the policy within the organization. Additionally, they need to stay informed about the latest trends in information security to regularly enhance and adjust the policy

# **External Resources Justifying the Policy**

* Compliance with industry standards like **PCI DSS** and **HIPAA** is critical to safeguard sensitive data and maintain the organization's integrity.
* Adherence to **PCI DSS** ensures the protection of payment card data and prevention of data breaches.
* Alignment with cybersecurity frameworks such as ***NIST*** Cybersecurity Framework and **ISO 27001** reinforces robust information security controls and resilience against evolving cyber threats.

Integration of these standards demonstrates the organization's commitment to **data** **protection**, **privacy**, and **security**, fostering trust among stakeholders and enhancing its credibility in the digital landscape.

# **Affirmative Procedure for Compliance**

* All personnel must **complete comprehensive information security training** upon onboarding and annually thereafter, covering topics such as threat identification, secure data handling, and confidentiality maintenance.
* Participants must showcase a full grasp of the organization's security protocols through interactive **workshops and real-world simulations**, demonstrating their ability to handle security incidents and adhere to data protection guidelines effectively.
* Policy violations can result in progressive **disciplinary actions, including warnings**, **additional training**, and **temporary access suspension**. In severe cases, the organization may pursue legal action or terminate contracts/employment, following established HR protocols for fairness and consistency. All actions will be documented to ensure transparency and accountability.

# **Frequency of Compliance Audits**

* Compliance with this policy will be audited **annually** to ensure comprehensive evaluation of the information security awareness and training program.
* **Random checks** and spot audits will be conducted **throughout the year** to assess immediate compliance and identify potential vulnerabilities.
* Annual audits will **cover** **the** **effectiveness of training materials**, participant engagement, and understanding of security protocols.
* Audit results will be **shared with relevant stakeholders**, including the **CISO**, **HR** department, and **senior management**, to facilitate informed decision-making and necessary adjustments to the training program

# **Specific Metric for Measuring Compliance**

* The compliance metric will be the **average score attained by employees**, contractors, and third-party vendors in information security awareness and training assessments.
* Assessments will encompass key performance indicators (**KPIs**) and qualitative and quantitative factors, evaluating theoretical understanding and practical application of security measures in simulated scenarios.
* **Simulations of real-world security incidents**, **interactive quizzes**, and **hands-on exercises** will be included in the assessments to assess participants' ability to identify, assess, and respond to potential security threats effectively.

# **Procedure for Collecting Compliance Metric**

* The **human resources department**, in collaboration with the information **security team,** will **oversee the administration of regular training sessions and assessments,** ensuring the active participation of all employees, contractors, and third-party vendors.
* The department will **maintain detailed records of participant attendance**, engagement levels, and performance throughout the training sessions and assessments, documenting individual **progress and achievements** in relation to the established learning objectives and performance standards.
* These records will **include data on attendance frequency**, participation in **interactive activities, scores achieved** in assessments, and any additional feedback provided by the participants during or after the training sessions.

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

* Responsible Party(ies) for Updating the Policy: The Information Security Department, overseen by the Chief Information Security Officer (**CISO**), plays a pivotal role in the **continuous review and updating** of the information security **awareness and training policy to ensure its alignment with evolving regulatory requirements, industry standards, and emerging cybersecurity threats.** The specific responsibilities of the Information Security Department in this context include:
* Conducting regular assessments of the policy's effectiveness and relevance, taking into account the **latest developments in the regulatory landscape,** technological advancements, and best practices in information security.
* Collaborating **closely** with the **legal department and compliance officers** to ensure that the **policy remains in full compliance with all relevant laws**, regulations, and industry standards, **thus** **minimizing legal risks** and liabilities for the organization.
* **Engaging with key stakeholders**, including **departmental managers**, **training facilitators**, and **employees**, to **gather feedback** and insights on the practical implementation of the policy and identify any challenges or areas requiring clarification or enhancement.

The Information Security Department, under the guidance of the Chief Information Security Officer, is committed to maintaining a robust and up-to-date information security awareness and training policy that safeguards the organization's assets, preserves its reputation, and fosters a culture of security consciousness and vigilance across all levels of the organization.

# **Frequency of Policy Review**

* The policy will undergo a comprehensive review annually to ensure its continuous alignment with the latest industry standards, emerging best practices, and evolving regulatory requirements in the field of information security. The **frequency of the policy review reflects the organization's commitment to maintaining a proactive approach to risk management** and its dedication to upholding the **highest standards of data protection and security**. The specific elements involved in the annual policy review process include:
* Conducting a thorough analysis of the evolving regulatory landscape and any updates or changes to relevant laws, standards, and compliance requirements that may impact the organization's information security practices and policies.

# **Procedure for Updating the Policy**

* The information security awareness and training policy will undergo a comprehensive review by the Chief Information Security Officer (**CISO**), in close coordination with the **legal department**, pertinent stakeholders, and subject matter experts. To ensure the thorough and efficient updating of the policy, a number of important steps and considerations will be included in the policy review process. Among these steps are:
* Conducting a detailed analysis of any **recent changes in regulatory requirements**, industry standards, and best practices in information security to identify potential gaps or areas in need of enhancement within the existing policy framework.
* Assessing the impact of technological advancements, emerging security threats, and evolving organizational structures on the current policy, seeking to integrate the **latest technological solutions** and security measures to fortify the organization's resilience against modern cyber threats.
* **Consulting** with relevant stakeholders, including departmental managers, training facilitators, and employees, to gather valuable feedback and insights on the practical implementation of the policy and identify any operational challenges or emerging security concerns that may necessitate policy adjustments or revisions.