Malta
Tourism Authority

MTA IT Dept Information Security

Policy Summary

Date: 19/09/2024
Version: 1.0
Department: Information Technology Department

Public

Document Control information

01. Document reference

Public- MTA Information Security Policy Summary -v1.0.doc

02. Document type

Policy

03. Security classification

Public

04. Synopsis

A summary detailing the Information Security Policy performed within Malta Tourism Authority (MTA) IT Department.

05. Document control

Author	Change Controller	Distribution Controller
Andrew Cassar Information Technology Department Manager	Godwin Camenzuli Information Technology Department Senior Manager	Marika Borg Information Technology Department Director

06. Authorisation

Issuing authority	Approval authority
Signature / Date Godwin Camenzuli ITD Senior	**Signature / Date** Marika Borg ITD Director

07. Modification history

Version	Date	Comments
Version 1.0	19/09/2024	First Version for suppliers

08. Acknowledgements

Involvement of MTA ITD personnel is acknowledged.

09. Distribution List

Public

10. References:

Table of Contents

01. Introduction

This Information Security Policy outlines the strategic direction and governance requirements for managing information security within the organization, aligning with ISO 27001:2022 standards. The policy's purpose is to protect the confidentiality, integrity, and availability of information and to prevent unauthorized access, disclosure, alteration, and destruction of information assets.

01.1 Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to the organization's information assets, including but not limited to digital data, printed documents, intellectual property, and information systems. The policy covers all aspects of information security within the organization, including physical, technical, and administrative controls.

01.2 Policy Objectives

The objectives of this Information Security Policy are to:

- Ensure compliance with ISO 27001:2022 and other relevant legal, regulatory, and contractual obligations.
- Protect the organization's information assets from security threats, whether internal or external, deliberate or accidental.
- Define roles and responsibilities for information security management within the organization.
- Establish a framework for risk assessment, incident response, and continual improvement in information security.
- Promote a security-conscious culture and provide regular training and awareness programs for all employees.

01.3 Information Security Management System (ISMS)

The organization has implemented an Information Security Management System (ISMS) based on ISO 27001:2022 standards to manage information security risks. The ISMS will be reviewed periodically to ensure its effectiveness and suitability in the ever-changing threat landscape.

01.4 Leadership and Commitment

Top management demonstrates leadership and commitment to information security by:

- Establishing and maintaining this Information Security Policy.
- Ensuring the integration of information security requirements into the organization's processes.
- Providing the necessary resources for the ISMS.
- Supporting information security initiatives and compliance efforts.
- Promoting a culture of information security awareness across the organization.

01.5 Information Security Roles and Responsibilities

- **IT Director:** Responsible for establishing, implementing, monitoring, and maintaining the ISMS. The IT Director ensures compliance with information security policies and procedures.
- **Information Security Committee**: Composed of senior management, IT, HR,, and other relevant departments. This committee oversees the development, implementation, and review of information security policies and initiatives.
- **All Employees:** Responsible for complying with information security policies, reporting security incidents, and participating in security awareness training.

01.6 Risk Management

A comprehensive risk management process is employed to identify, assess, and treat information security risks. This process includes:

- **Risk Assessment:** Identifying and evaluating risks to information assets.
- **Risk Treatment:** Implementing appropriate controls to mitigate identified risks.
- **Risk Acceptance:** Accepting residual risks based on the organization's risk appetite and tolerance.
- **Risk Review:** Regularly reviewing and updating risk assessments to address changes in the threat landscape and business operations.

01.7 Asset Management

- **Inventory of Assets:** The organization maintains an up-to-date inventory of information assets, including hardware, software, data, and documentation.
- **Asset Classification:** Information assets are classified based on their value, sensitivity, and criticality to the business.
- **Acceptable Use**: Employees are informed of the acceptable use of information assets through formal policies, including guidelines for using email, internet, mobile devices, and removable media.

01.8 Access Control

- **Access Rights:** Access to information assets is granted based on the principle of least privilege, ensuring individuals only have access necessary to perform their roles.
- **Authentication and Authorization:** Robust authentication mechanisms, including multi-factor authentication (MFA), are used to verify user identities and control access to sensitive information.
- **User Management:** User accounts, privileges, and access rights are managed systematically, including procedures for onboarding, role changes, and termination.

01.9 Cryptography

- **Encryption:** Sensitive data, whether at rest or in transit, is encrypted using industry-standard cryptographic algorithms.
- **Key Management:** Cryptographic keys are managed securely throughout their lifecycle, from generation to destruction, in line with industry best practices.

01.10 Physical and Environmental Security

- **Secure Areas:** Access to physical locations housing critical information assets, such as data centres, is restricted and monitored.
- **Protection Against Environmental Threats:** Appropriate measures (e.g., fire detection and suppression systems, climate control) are implemented to protect information assets against environmental risks.

01.11 Operations Security

- **Change Management**: All changes to information systems are reviewed, approved, and documented to ensure they do not compromise security.
- **Malware Protection**: Anti-malware software is installed and maintained on all systems to protect against viruses, spyware, ransomware, and other malicious code.
- **Backup:** Regular backups of critical data are performed and stored securely to ensure availability in the event of data loss.

01.12 Communications Security

- **Network Security:** Security measures, including firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs), are implemented to protect the integrity and confidentiality of information communicated over networks.
- **Data Transfer:** Sensitive data is transmitted securely using encryption and secure communication channels (e.g., SSL/TLS).

01.13 14. Supplier Relationships

- **Supplier Risk Assessment:** The security posture of suppliers is assessed to ensure they meet the organization's information security requirements.
- **Contracts and Agreements:** Contracts with suppliers include clauses that require adherence to information security policies and the handling of information securely.

01.14 Information Security Incident Management

- **Incident Response:** The organization has an incident response plan for promptly addressing information security incidents, including detection, analysis, containment, eradication, and recovery.
- **Reporting:** Employees are encouraged to report security incidents or suspected breaches to the designated point of contact without delay.
- **Incident Review:** Post-incident reviews are conducted to identify root causes and implement corrective actions to prevent recurrence.

01.15 16. Business Continuity Management

- **Business Continuity Planning**: The organization maintains a business continuity plan (BCP) to ensure the availability of information and information systems during disruptive events.
- **Disaster Recovery:** Disaster recovery procedures are established to restore critical systems and data in the event of an incident affecting the IT infrastructure.

01.16 Compliance

- **Legal and Regulatory Compliance:** The organization identifies and complies with applicable legal, regulatory, and contractual obligations related to information security.
- **Internal Audits:** Regular internal audits are conducted to assess the effectiveness of the ISMS and identify areas for improvement.
- **Non-Compliance:** Non-compliance with this policy or related information security procedures may result in disciplinary action, up to and including termination.

01.17 Human Resource Security

- **Pre-Employment:** Background checks are conducted for potential employees to assess their suitability for positions that handle sensitive information.
- **Training and Awareness:** All employees receive information security training during onboarding and periodic refresher training.
- **Termination:** Procedures are in place to manage the secure exit of employees, including revoking access to information assets and recovering company-owned equipment.

01.18 Continual Improvement

The ISMS and this Information Security Policy are subject to continuous improvement through regular monitoring, review, and audit processes. Feedback mechanisms are in place to ensure that lessons learned from incidents, audits, and assessments are incorporated into policy updates and control implementations.

01.19 Review and Revision

This Information Security Policy is reviewed annually, or more frequently, if necessary, to reflect changes in the threat environment, technology, legal and regulatory requirements, or business operations.

01.20 Policy Acceptance

All employees, contractors, and third parties with access to information assets must acknowledge their understanding of, and agreement to comply with this Information Security Policy summary.

01.21 Document Control

This document is maintained as part of the ISMS documentation and is subject to version control to track changes and revisions.