Marquistech

Marquis Technologies - Physical Security Policy

Function	:	Corporate Security
Doc Ref	:	MQT/ISMS/A7.1/CP/01
Approver	:	Deven Potdar
Version & Status	:	1.1, Approved

Revision History

Version	**Reviewer**	**Date**
1.0	Deven Potdar	01.12.2024

1 Purpose

All corporate area and assets must be adequately protected. Personnel security is a necessary building block for safeguarding assets. This policy defines requirements for protection of Marquis Technologies corporate assets from intentional abuse, misuse, or destruction by employees, contractors, or consultants.

The protection of the physical environment is one of the most obvious yet most important tasks within the area of information security. A lack of physical access control can undo the most careful technical precautions and potentially put lives at risk.

Marquis Technologies is committed to ensuring the safety of its employees, contractors and assets and takes the issue of physical security very seriously. This policy sets out the main precautions that must be taken and, together with the supporting documented listed, forms a significant part of our Information Security Management System (ISMS).

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Marquis Technologies systems.

2 Scope

This policy applies to all employees, contractors, and consultants who handle Marquis Technologies assets including sensitive information or sensitive information entrusted to Marquis Technologies.

3 Policy Statement

Asset protection is addressed at the recruitment stage, included in the employee contracts, and monitored during an individual 's employment. To ensure compliance with policy objectives, these statements must be followed:

3.1 Requirement to Protect Corporate Assets

3.1.1 All employees, contractors, and consultants must protect both tangible and intangible corporate assets.

3.1.2 All employees, contractors, and consultants are responsible for reporting to the appropriate manager any real or suspected threats to corporate assets.

3.2 CCTV Surveillance and Access control

3.2.1 We are currently using number of cameras at different locations covering:

- Reception

- All passage
- One in every test lab and rooms
- Inventory

3.2.2 CCTV Data is stored for 60 days, it can be increased based on client needs

3.2.3 CCTV footage in routinely monitored by Corporate Security.

3.2.4 Access to every room is restricted by access card system.

3.3 Access Control

3.3.2 All employees must use their assigned access cards to gain entry to the premises and designated areas.

3.3.3 Visitors must sign in at the reception area, provide identification, and wear visitor badges at all times.

3.3.4 Access to sensitive areas, such as server rooms or data centers, is restricted to authorized personnel only.

3.3.5 Sensitive areas, including server rooms and data centers, will have controlled access with card-based or biometric authentication.

3.3.6 Critical equipment, such as servers or network devices, will be physically secured to prevent tampering.

3.4 Alarm Systems:

3.4.1 Intrusion detection systems and alarms will be installed to detect unauthorized access attempts and trigger alerts.

3.4.2 Alarms will be connected to a central monitoring station for prompt response and notification of security personnel.

3.5 Security Incidents

Ensure security incidents and policy violations are escalated appropriately.

3.5.1 The Security Officer will implement a system for security incident reporting, response, tracking, and resolution as per Incident Response policy

3.5.2 All employees and contractors are responsible for reporting to the appropriate manager any violations of policy or other directives promptly.

3.6 Compliance and Auditing:

3.6.1 Regular audits will be conducted to assess compliance with physical security policies and identify areas for improvement.

3.6 .2 Compliance with applicable laws, regulations, and industry standards will be ensured.

3.7 Paper & equipment security:

3.7.1 Paper based (or similar non-electronic) information must be assigned an owner and a classification. Appropriate information security controls must be put in place to protect it according to the provisions in the *Asset Handling Procedure*.

3.7.2 Paper in an open office must be protected by the controls for the building and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a secure area protected by access controls

3.7.3 All general computer equipment must be in suitable physical locations that:

- Limit the risks from environmental hazards – for example heat, fire, smoke, water, dust and vibration
- Limit the risk of theft – e.g. if necessary, items such as laptops should be physically attached to the desk
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorized people

3.7.4 Data must be stored on network file servers or approved cloud locations where available. This ensures that information lost, stolen or damaged via unauthorised access can be restored and its integrity maintained.

3.7.5 All servers located outside of the data centre in Marquis Technologies premises must be sited in a physically secure environment.

3.7.6 Business critical systems must be protected by an Un-interruptible Power Supply (UPS) to reduce the operating system and data corruption risk from power failures.

3.7.7 All items of equipment must be recorded in the Marquis Technologies inventory. Procedures must be in place to ensure the inventory is updated as soon as assets are received or disposed of.

3.7.8 All equipment must be security marked and have a unique asset number allocated to it. This asset number must be recorded in the Marquistech inventory.

3.7.9 Cables that carry data or support key information services must be protected from interception or damage.

3.7.10 Power cables must be separated from network cables to prevent interference. Network cables must be protected by conduit and where possible avoid routes through public areas.

3.8 **Equipment lifecycle management:**

Marquis Technologies and third-party suppliers must ensure that all of Technologies' IT equipment is maintained in accordance with the manufacturer's instructions and any documented internal procedures to ensure it remains in effective working order.

3.8.1 Staff involved with maintenance must:

- Retain all copies of manufacturer's instructions
- Identify recommended service intervals and specifications
- Enable a call-out process in event of failure
- Ensure only authorized technicians complete any work on the equipment
- Record details of all remedial work carried out
- Identify any insurance requirements
- Record details of faults incurred and actions required

3.8.2 A service history record of equipment must be maintained so that decisions can be made regarding the appropriate time for it to be replaced.

3.8.3 Manufacturer's maintenance instructions must be documented and available for support staff to use when arranging repairs.

3.8.4 The use of equipment off-site must be formally approved by the user's line manager.

3.8.5 Equipment that is to be reused or disposed of must have all its data and software erased / destroyed. If the equipment is to be passed onto another organization (for example returned under a leasing agreement) data removal must be achieved by using approved, appropriately secure software tools.

3.8.6 Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process must confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.

3.8.7 Loading areas and holding facilities must be adequately secured against unauthorised access and all access must be auditable.

3.8.8 Subsequent removal of equipment must be via a formal, auditable process.

3.8.9 Information security arrangements must be subject to regular independent audit and security improvements recommended where necessary.

4 Responsibilities

Corporate Security is responsible for implementing the educational requirements of this policy.

5 Compliance

5.1 Company officers and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

5.2 Company line managers have the responsibility to enforce compliance with this policy.

5.3 Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Marquis Technologies