Marquistech – Access Control Policy

Owner	:	Information Security Officer
Reviewer	:	Sudarshan Kadam
Approver	:	Deven Potdar
Version & Status	:	1.5, Approved

1. Purpose

Physical and electronic security is essential in providing security, access, and protection to Marquistech's personnel, equipment, buildings, and resources. Access to Marquistech's assets is a privilege, not a right, and implies user responsibilities and accountability.

The purpose of this policy is to regulate access to Marquistech property and ensure that any individual, department, operating unit, or program within the scope of this policy is aware of their respective responsibilities. This policy will help provide a safe and secure environment through the diligent control of electronic access devices.

2. Scope

This policy applicable to all employees, contractors, and consultants who handle Marquistech assets including those who have access to sensitive information or sensitive information entrusted to Marquistech.

3. Policy

All Users, who use the Marquistech's information assets and information systems, will be responsible for safeguarding those resources and the information the information Owners hold, from disruption or destruction.

Access allocation will be monitored to ensure compliance with this Access Control Policy.

- Access cards are given to employees in the office, which is restricted based on project based need.
- IT Team will check the validity of all user access requests to information assets owned by them before implementation.
- All resources use personally identifiable accounts when access any system or host.
- IT Team will ensure that all access privileges held by all end-user accounts has a documented and valid business justification approved by senior management.
- IT Team monitors all Access allocation on continuous basis. All guest access are also monitored.
- Human Resources (HR) will inform the IT department of all Employee/Contractor movement (Joining/Exit of employees).
- Users should not share access codes and/or passwords, if access to other information systems are required then a formal request should be put forward for authorisation by an appropriate manager.
- Users should not share their physical access cards; if physical access to restricted areas is required then a formal request should be put forward for authorisation by the line manager.

- Users should be responsible for the security (and secrecy) of their own secret authentication information. In no circumstances is secret authentication information to be shared.
- Users should ensure incidents are reported and escalated in-line with the Marquistech' s Security Incident Management Procedure.
- All guest visits are logged and details of logs retained for a minimum of one month, unless otherwise restricted by law.
- Access to information assets is restricted to authorised employees or contractors and is protected by appropriate physical and logical authentication and authorisation controls.
- All information stored on systems and hosts is protected with file system, network share, application, or database specific access control lists and no sensitive personal data is available to read-only authenticated end-users or world-readable.
- Users are authenticated to information systems using accounts and passwords.
- Access privileges is authorized by the appropriate Manager and allocated to employee, based on the minimum privileges required to fulfil their job function.
- Administrator accounts is only granted to those users who require such access to perform their job function. Administrator accounts is strictly controlled and their use is logged, monitored and regularly reviewed.
- Access privileged are immediately revoked in case of employee termination.
- Any re-joining staff must reapply for all access and privileges to systems and hosts.
- Access privileged are immediately revoked if required by client.
- Access privileged are immediately revoked if any breach of policy is found.
- All third party access (Contractors, Business Partners, Consultants, Vendors) should be authorised by an appropriate Manager in advance.

4. Responsibilities

- IT Department and Corporate Security is responsible for monitoring and enforcing the policy.
- Annually review the Access Control processes, standards and procedures, to achieve compliance with this Access Control Policy.

5. Revision History

Version	Reviewer	Date
1.6	Deven Potdar	10 April, 2025
1.5	Sudarshan Kadam	05 April, 2024
1.4	Deven Potdar	20 April, 2023
1.3	Sudarshan Kadam	05 February, 2022
1.2	Deven Potdar	10 February, 2021
1.1	Sudarshan Kadam	10 September, 2020
1.0	Deven Potdar	2 October, 2019