Marquistech – Information Security Policy

Owner	:	Abel Subhash (Information Security Officer)
Reviewer	:	Sudarshan Kadam
Approver	:	Deven Potdar
Version & Status	:	1.6, Approved

Marquistech

Table of Contents

1. Purpose

Marquistech must safeguard restricted, confidential or sensitive information/data loss to prevent harming our company's reputation and to avoid seriously impacting our clients. It is a critical business requirement to keep information protected along with having flexible access to data. User awareness is the primary objective to avoid accidental loss.

This Policy document includes all aspects of security of confidential information and must be informed to all Marquistech employees. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees where applicable.

2. Scope

Any and all employees, contractors and individual with access to Marquistech systems or information are responsible of protecting the data.

3. Policy statement

3.1 All employees and contractors need to complete Marquistech' security awareness training and agree to uphold the acceptable use policy.

3.2 Employees are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by Marquistech. For example, the use of external e-mail systems not hosted by Marquistech to distribute data is not allowed.

3.3 Employees should always keep a clean desk. To maintain information security you need to ensure that all printed in scope data is not left unattended at your workstation.

3.4 Employees need to use a secure password on all company systems as per the password policy. These credentials must be unique and must not be used on other external systems or services. Passwords are automatically changed every 30 days for both Laptop and email system.

3.5 Terminated employees will be required to return all records, in any format, containing personal information.

3.6 Employees must immediately notify Corporate Security and Managers in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc).

3.7 If the system is not locked by the user, it will auto locked after 15 mins of inactivity, to avoid unauthorized access.

3.8 If employees have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from Corporate Security if you are unsure as to your responsibilities.

3.9 Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.

3.10 Data that must be moved within company is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). Marquistech will provide or guide you with systems or devices that fit this purpose. No online data transfer to external websites, FTP or peer to peer are allowed. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with IT Department.

3.11 Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from IT Department.

3.12 When in public, employees should protect information. Do not discuss confidential information in public areas (airport lounge, café, on road etc.)

3.13 Employees need to adhere to following for social media pages/handles, it is pertinent to follow the below guidelines:

- Never post any malicious, misleading, derogatory, obscene, defamatory, threatening, racially discriminating, or religiously unacceptable content on the Company's or personal Social Media platforms.
- Never share information that is confidential and proprietary about the Company, including but not limited, to the company device details, project information, contact list, trademarks, upcoming product releases, marketing plans/campaigns, sales data, finances, customer details, company strategy, and any other information that has not been publicly released by the company.
- Never use an official email id for personal social media accounts.
- Never comment about any Company/Group related legal matters, customer grievances, regulatory issues, or litigation nor communicate anything that might damage the Company's reputation.
- Never indulge in personal conversations with family/friends on the Company's official page/platforms.
- If an employee identifies himself/herself as an Marquistech employee on their social media handles, it should be clear that the views expressed are not necessarily those of the Company.
- Always take the approval of other employees before posting their photos/videos on the Company's social media platforms.
- If an employee has any grievances, they should be taken up through the Company's established protocols only and should not be posted on social media platforms.
- If an employee becomes aware that material posted on any social media site is inconsistent with the Company's social media guidelines, it must be immediately reported to the company
- Never use the Company's logo or company branding on any of the social media platforms without prior approval.
- It is a good practice to restrict using the name of the Company at professional networking sites only.
- Never create a social media page in the name of the Company.
- In case any customer approaches you via social media regarding their query/grievance, please do not respond without consulting the project manager.

3.14 Data on all system (e.g. laptops) are encrypted both in transit and in rest.

3.15 All computer software or data developed by Marquistech' employees or contractors on behalf of Marquistech or licensed for Marquistech use is the property of Marquistech and may not be copied for use at home or any other location, unless approved by management.

3.16 Antivirus system approved by IT Department must be installed in systems, which should scan all electronic files for viruses. Users are not authorized to turn off or disable antivirus. Antivirus we deploy, implements Deep Guard engine which monitor and eliminate malicious file.

3.17 For network security, only ports for official purpose are allowed and monitored.
3.18 All systems must have most recent OS update and patches.
3.19 Operational software should be downloaded through legal and verified channels. Installation of software unrelated to operations is prohibited.
3.20 The email system is enabled with Anti Phishing and Anti Spamming settings.
3.21 Every server for data storage has a backup server to maintain redundancy.
3.22 Physical and electronic access to confidential information, devices and systems are controlled. Access is provided on "need to know" basis. Authentication is done with User ID and password.
3.23 IT Department is available for support 24/7, either remotely or in person.

4. Compliance
4.1 Corporate Security is responsible to ensure the compliance to security policies.
4.2 Company officers and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
4.3 Company line managers have the responsibility to enforce compliance with this policy.
4.4 Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

5. Documentation Review and Revision History

Version	Reviewer	Date
1.0	Kailash Lalwani	02-10-2019
1.2	Deven Potdar	05-11-2020
1.3	Deven Potdar	10-11-2021
1.4	Sudarshan Kadam	11-05-2022
1.5	Deven Potdar	08-05-2023
1.6	Sudarshan Kadam	24-05-2024
1.6	Deven Potdar	21-05-2025