Acceptable Use Policy

DOCUMENT CLASSIFICATION	Restricted
DOCUMENT REF	MQT/ISMS/A5.10/CP/02
VERSION	01
DATED	01/12/2024
DOCUMENT AUTHOR	Abel Subhash
DOCUMENT OWNER	Deven Potdar

Revision history

VERSION	DATE	Reviewer	Page No	SUMMARY OF CHANGES

Contents

1 Introduction

Marquis Technologies takes the subject of information security very seriously. We have a duty to protect the information that we collect and use for the benefit of the organization and its customers. As an employee, you will be expected to comply fully with all of the information security policies that are in place and to report any breaches of these policies of which you may become aware.

This document gives a summary of the main points of the relevant policies, and you will be asked to sign to say that you have read it and understand its provisions. Where your role involves tasks or access to information that are the subject of a more detailed topic-specific policy, you will be made aware of your additional responsibilities as part of your induction for the role.

Anyone breaching information security policy may be subject to disciplinary action. If a criminal offence has been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, please seek advice from your immediate manager in the first instance.

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.

The following topic-specific policies and procedures are relevant to this document:

- *Information Security Policy*
- *Electronic Messaging Policy*
- *Internet Access Policy*
- *Mobile Device Policy*
- *BYOD Policy*
- *Remote Working Policy*
- *Privacy and Personal Data Protection Policy*
- *Cloud Services Policy*
- *Asset Handling Procedure*
- *Software Policy*
- *Access Control Policy*
- *Anti-Malware Policy*
- *Information Security Incident Response Procedure*
- *IP and Copyright Compliance Policy*
- *Social Media Policy*
- *HR Security Policy*
- *Asset Management Policy*

2. Acceptable Use:

Please ensure you have read and understood the following summary of the main points of the Marquis Technologies policies regarding information security.

1.1 General

You are expected to make yourself familiar with, and follow, the organization's security policies and procedures and any special instructions relating to your work.

Be aware that your use of Marquis Technologies computer and communications systems may be monitored and/or recorded for lawful purposes.

You must always comply with the legal, statutory or contractual obligations that the organization informs you are relevant to your role.

1.2 Access Control

You are responsible for the use and protection of the user credentials with which you are provided (user account and password, access token or other items you may be provided with).

Use strong passwords that comply with organization policies and take reasonable precautions to ensure that your passwords are only known by you (for example, not sharing passwords or writing them down).

Don't use the same password (or close variation of the same password) for multiple user accounts.

Never use anyone else's user account and password to access the organization's systems.

You must not use privileged user accounts (user accounts with higher-than-normal system access) for business-as-usual activities.

You must not attempt to access any computer system to which you have not been given authorised access.

Never attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.

You must not connect unauthorised devices to the organization network.

1.3 Classified information

Ensure that you label any classified material that you create appropriately according to published guidelines so that it remains appropriately protected.

Always protect any classified material you send, receive, store or process according to the level of classification assigned to it, including both electronic and paper copies.

Don't send classified information over the Internet via email or other methods unless appropriate methods (for example encryption) have been used to protect it from unauthorised access.

Always ensure that you enter the correct recipient email address(es) so that classified information is not compromised.

Take care that you are not overlooked by unauthorised people when working and exercise appropriate precautions when printing classified information.

Securely store classified printed material and ensure it is correctly destroyed when no longer needed.

Never leave your computer unattended such that unauthorised access can be gained to information via your user account while you are away from your workstation.

On leaving the organization, you must inform your manager prior to departure of any important information held in your user account or in a location to which the organization has no, or limited, access.

1.4 Electronic messaging

Electronic messaging covers email and various forms of instant and store-and-forward messaging such as SMS texts, messaging apps, web chats and messaging facilities within social media platforms.

The organization-provided electronic messaging facilities must always be used when communicating with others on official business. You must not use a personal account for this purpose.

All organization messages should be considered to be official communications from the organization and treated accordingly.

You must not send messages containing material, which is defamatory, obscene, does not comply with the organization's equality and diversity policy or which a recipient might otherwise reasonably consider inappropriate. In particular, organization electronic messaging facilities must not be used:

- For the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organizations
- To send material that infringes the copyright or intellectual property rights of another person or organization

- For activities that corrupt or destroy other users' data or otherwise disrupt the work of other users
- To distribute any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- To send anything which is designed or likely to cause annoyance, inconvenience or needless anxiety to others
- To convey abusive, threatening or bullying messages to others
- To transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs
- For the transmission of defamatory material or false claims of a deceptive nature
- For activities that violate the privacy of other users
- To send anonymous messages - i.e. without clear identification of the sender
- For any other activities which bring, or may bring, the organization into disrepute

If you are not sure whether your intended message falls into this category, please consult your line manager before sending.

You should be aware that many information security breaches occur as a result of "phishing", where an email or other type of message is sent which either has a malicious attachment or includes links to websites which are set up to steal information. If you are suspicious about a message, report it to the service desk without opening any attachments or clicking on links.

1.5 Internet browsing

Your Internet access on organization-owned devices is primarily provided for tasks reasonably related to your work including:

- Access to information and systems that is pertinent to fulfilling the organization's business obligations
- The capability to post updates to organization-owned and/or maintained web sites and social media accounts
- An electronic commerce facility (e.g. purchasing equipment for the organization)
- Research
- Other tasks that are part of your job role

The organization permits personal use of the Internet in your own time (for example during your lunchbreak), provided it does not interfere with your work. Any exception to this is at the discretion of your line manager.

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must not use the Internet access provided by Marquis Technologies to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files
- Subscribe to, enter or utilise real time chat facilities
- Subscribe to, enter or use online gaming or betting sites
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business
- Download any software that does not comply with the organization's software policy

The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material will include data, images, audio files or video files the transmission of which is illegal and material that is against the rule, essence and spirit of this and other organizational policies.

You must also avoid websites that are flagged by anti-malware or browser software as being potentially unsafe, or which appear suspicious.

1.6 Mobile devices

Mobile devices include items such as laptops, notebooks, tablet devices, smartphones and smart watches.

Unless specifically authorized, only mobile devices provided by the organization may be used to hold or process classified information.

An organization-provided device is for your business use only; it must not be shared with family or friends or used for personal activities.

You must not remove equipment or information from the organization's premises without appropriate approval.

You must take precautions to protect all mobile devices and computer media when carrying them outside the organization's premises (for example, not leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft).

The device must not be connected to non-corporate networks such as public Wi-Fi or the Internet.

Do not remove any identifying marks on the device such as a company asset tag or serial number. Ensure that the device is locked away when being stored and that the key is not easily accessible.

Do not add peripheral hardware to the device without approval.

Permission must be obtained before the device is taken out of the country. This is to ensure that it will work and to consider any insurance implications.

Where possible, the device will be secured so that all of the data on it is encrypted and so is only accessible if the password is known. If the device is supplied with encryption, do not disable it.

1.7 Privacy and compliance

Marquis Technologies has a legal obligation to comply with all applicable legislation affecting its business operations, and every employee must play their part in meeting these requirements, in areas such as data privacy, intellectual property, and governance.

You must ensure that you follow organization policies and rules for the processing of personal data at all times.

Take care to understand the rules surrounding the use of the intellectual property of others, such as software, videos, music, books, documentation, photographs and logos so that copyright and other protections are not infringed.

Ensure that the intellectual property of Marquis Technologies is protected when dealing with third parties.

1.8 Cloud computing

Marquis Technologies makes extensive use of cloud services to enable business processes in a responsive and flexible way. These services are subject to a due diligence procedure to ensure that they meet our business, security and legal requirements.

As part of your job role, you must only make use of cloud services that have been put in place by Marquis Technologies. The storing of classified information in unapproved cloud services is strictly prohibited.

1.9 Use of social media

Marquis Technologies makes extensive use of social media to communicate directly with our customers as part of our marketing activity, to provide support for our products and services, and to obtain useful feedback on how our organization is perceived.

You must be authorised to use corporate social media accounts and to represent the organization to the public, and only if that is part of your job role.

Only authorised accounts should be used to publish messages and respond to other users of relevant social media channels. Do not use your own personal accounts.

Marquis Technologies respects your personal online activity as a medium of self-expression, but remember you continue to have responsibilities to the organization outside of working hours.

When using social media to engage on matters relevant to Marquis Technologies, make it clear it is your own opinion you are expressing and not that of the organization.

1.10 Information security incidents

If you detect, suspect, or witness an incident that may be a breach of security, or if you observe any suspected information security weaknesses in systems or services, you should in the first instance inform your line manager, or contact the IT Team.

Unusual or unexplained events, such as messages appearing on your device, can indicate that an incident is happening, and these should be reported as soon as possible.

If an incident is detected by Marquis Technologies, you may be asked to take specific action, such as logging off systems or closing your device down. You should comply with such requests as soon as possible.

1.11 Malware protection

Your device will be protected by organization-supplied anti-malware software.

You must not attempt to disable anti-malware protection provided to protect your device.

You must take care not to introduce viruses or other malware into the system or network, for example by inserting unknown peripherals or media into your device.