metclad
contracts

M33 - Security Policy

IT Systems and communications

Purpose of Policy

Ensure that all members of staff are aware:

- Of possible security threats and understand what is required if there is a security breach.
- Of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access.

Scope

This Information Systems Security Policy applies to ALL members of staff and has been written in a simple and clear manner.

Policy

Awareness and Communications

All authorised members of staff will be informed of the policy and of supporting policies and guidelines when their account is issued. Updates to guidance will be carried out at team meetings and via internal communications.

Breaches of policy must be reported by anyone aware of the breach in a timely manner to the office manager or

All members of staff will be made aware of the security software installed on their devices that will protect them from:

- Computer Viruses
- Ransomware
- Social Engineering attacks
- Malware
- Malicious Websites
-

Password Control

Passwords are changed regularly and must contain Numbers, Letters (Upper and Lowercase) and Symbols.
Members of staff must not write down their passwords or store them electronically.
Microsoft Office 365 account two factor authentication in place.

Information Protection

- Information will be protected against unauthorised access and processing.
- Information will be protected against loss and corruption.
- Electronic communications will be encrypted.

Compliance and Incident notification

It is vital that members of staff comply with the information security policy.
Any breach of information security is a serious matter and could lead to the possible loss of confidentiality, integrity, or availability of personal or other confidential data. Such a loss may result in criminal or civil action against Metclad Contracts Ltd and the loss of business and financial penalties.

Any actual or suspected breach of this policy must be notified to Senior Management at the earliest possible opportunity. All security incidents will be investigated, and consequent actions may follow.

Data Security

Company Data is only stored on the file server in the correct folder. The data drive is mirrored (RAID01) with enterprise level SAS hard disk drives. All company data is backed up to external hard drives, which one is stored offsite.

The network is protected by a Cisco ASA firewall and all Servers and PC's have Eset Anti-Virus software installed on them. Software patching is carried out live.

Cloud based solutions Dropbox, iAuditor, HandS HQ, Breathe all have at least similar levels of security to our inhouse server.

Home Working

In the unlikely event of the employee being required to work from home, the individual is required to relocate their office equipment that is essential to their job duties, like laptops, desktops, monitors, headsets and phones (when applicable.)

We will install VPN and company-required software when employees relocate their equipment.

We will not provide secondary equipment (e.g. printers and additional screens.)

Any necessary additional cables & adaptors , within reason, will be provided by the company.

Equipment that we provide is company property.

When working from home Microsoft Teams must be unlisted & logged on during working hours, it is recommended employees add this to their "startup" programs list.

Employees must keep equipment safe and avoid any misuse. Specifically, employees must:

- Keep their equipment password protected.
- Store equipment in a safe and clean space when not in use.
- Follow all data encryption, protection standards and settings.
- Refrain from downloading suspicious, unauthorized or illegal software.

Responsibilities

Members of staff must:

- Adhere to the Acceptable Use Policy and follow relevant supporting procedures and guidance.
- Should only access systems and information they have a legitimate right to and not knowingly attempt to gain illegitimate access to other information.
- Must not aid or allow access for other individuals in attempts to gain illegitimate access to data. In particular individuals should adhere to the information security 'dos and don'ts' outlined in the table below:

DO	DO NOT
Do use a strong password and change it if you think it may have been compromised	Don't give your password to anyone
Do report any loss or suspected loss of data	Don't reuse your password for any other account
Do be on your guard for fake emails or phone calls requesting confidential information - report anything suspicious to Senior Management	Don't open suspicious documents or links
Do keep software up to date and use antivirus on all possible devices	Don't undermine the security of Metclad Contracts Ltd's systems
Do be mindful of risks using public Wi-Fi or computers	Don't provide access to Metclad Contracts Ltd's information or systems
Do ensure Metclad Contracts Ltd's data is stored on Metclad Contracts Ltd's systems	Don't copy confidential Metclad Contracts Ltd's information without permission
Do password protect and encrypt your personally owned devices	Don't leave your computers or phones unlocked

Record of Changes to this Document

Issue No.	Date of Issue	Summary of Changes
01	September 2020	Home working section added to compliment office RAMS (CV19)
02	September 2021	No changes
03	January 2023	Tweaks to wording added MS two factor authentication