D.M.H INTERIORS LTD
PARTITION/CEILINGS PLASTERING SPECIALIST

2/23/2023

Approved by:	**Darren Hancock M.D**
Last reviewed on:	**February 2023**
Next review due by:	**January 2024**

Policy Brief & Purpose

DMH Interiors Limited Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become, to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise our reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks, which we have outlined in this policy.

Scope

This policy applies to all our employees, contractors, and anyone who has permanent or temporary access to our systems and hardware.

Policy Elements - Confidential Data

Confidential data is secret and valuable. Common examples are:

- Information concerning clients, contractors, and staff
- Unpublished financial information and contractual data

All employees are obliged to protect this data. In this policy, we will give our staff instructions on how to avoid security breaches.

Protect Personal and Company Devices

When staff/contractors use their digital devices to access emails or accounts, they introduce security risk to our data. We advise staff/contractors to keep both their personal and work-issued devices secure. They can do this if they:

- Keep all devices password protected.
- Ensure antivirus software is kept up to date.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees/contractors to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Keep Emails Safe

Emails often host phishing attacks, scams, or malicious software (e.g., trojans and worms.) To avoid virus infection or data theft, we instruct employees/contractors to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g., offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email, they received is safe, they should contact our IT provider.

Manage Passwords Properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g., birthdays).
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person is not possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords regularly, but at a minimum every six months.

Transfer Data Securely

Transferring data introduces security risk. Employees/Contractors must:

- Avoid transferring sensitive data (e.g., client information, financial records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees seek the support of IT.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisation have adequate security policies.
- We encourage employees/contractors to reach out to our IT/administration with any questions or concerns.

Additional Measures

To reduce the likelihood of security breaches, we also instruct our employees/contractors to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to our administration team (Sam Jones)
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, Unauthorised, or illegal software on their DMH equipment.
- Avoid accessing suspicious websites.

Our IT Team Will:

- Install firewalls, anti-malware software and access authentication systems.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.

Our company will have all physical and digital shields to protect information.

Remote Employees and Contractors

Remote employees must follow this policy's instructions as well. Since they will be accessing DMH's information and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Disciplinary Action

We expect all our employees/contractors to always follow this policy and those who cause security breaches may face disciplinary action or if a contractor dismissed.

Examples of deliberate or serious breaches of this policy and examples of misuse are, but not limited to:

- Knowingly disclose login information to an unauthorised third party
- Inappropriate disclosure of personal data
- Knowingly installing software on DMH devices that hasn't been approved by DMH which leads to a breach.
- Allowing the use of DMH devices by unauthorised third parties
- Storing data on insecure media such as removable media that leads to a breach.

Take Security Seriously

Everyone should feel that their data is safe. We can all contribute to this by being vigilant and keeping cyber security at the top of our minds.

Reporting and Contact Information

Questions or reports relating to this policy should be addressed to:

Janice Saunders – Office Manager –janice@dmhinteriors.com

Sam Cooper – Administration –sam@dmhinteriors.com

Jon Withers– External IT Support –jwithers@enhancedgroup.co.uk

Darren Hancock

Managing Director

23rd February 2023