IT Security Policy

Introduction and Purpose

The Michael Lonsdale Group inclusive of Michael Lonsdale Ltd, Michael J Lonsdale Ltd, Michael J Lonsdale (Electrical) Ltd and E7 Building Services Ltd (The Michael Lonsdale Group) has produced this IT Security document to provide a structured approach to managing information security risks within our group.

These policies have been adopted by the Michael Lonsdale Group following the increased regulatory attention to the process of protecting information by preventing, detecting, and responding to the loss of data, including personal data, sensitive personal data, company data, client data, client work products, and sub-contractor data.

The approaches outlined include protecting the integrity of such information and the computing environments within the organisation, including the devices that store, process, and transmit sensitive data (for example, workstations, laptops, servers, mobile devices, applications, databases, file stores, etc), by minimising unauthorised access to the data and any network the Michael Lonsdale Group devices are connected to.

Scope

This policy applies to the employees (full-time, part-time or casual) and subcontractors (Associates) of the Michael Lonsdale Group who have or are responsible for an account (or any form of access that supports or requires a password) on any the Michael Lonsdale Group owned or leased IT system that resides either in or outside of the domain network.

This document is also applicable to other stakeholders in the Michael Lonsdale Group.

The Michael Lonsdale Group policy and procedure documents may be distributed to suppliers, accreditation and compliance bodies and any other relevant third parties.

In some cases, third parties such as suppliers or those performing on-site work for the Michael Lonsdale Group will be expected to adhere to our policies, which will be made available where applicable.

Hardware Scope

The Michael Lonsdale Group IT systems are built on a hybrid system, of virtual and physical servers, laptop and desktop computers and mobile devices inclusive of iOS and Android tablets and mobile phones.

Responsibilities

All systems at the Michael Lonsdale Group are managed by our third-party Managed Services Provider (MSP) D H Technical Services Limited (DHTS) with oversight from the Michael Lonsdale Group Senior Managers.

Senior Managers are responsible for ensuring that DHTS is given the correct instructions for managing our IT systems.

Employees and Subcontractors must:

- Agree to comply with the policies and procedures related to IT security contained in this document.
- Adhere to confidentiality and non-disclosure obligations.
- Acknowledge that violations of the Michael Lonsdale Group policies and procedures may result in disciplinary action, up to and including dismissal or civil or criminal proceedings.
- Complete any mandatory training.
- When leaving the Michael Lonsdale Group, return any equipment, property, and sensitive data.
- Be aware of where you leave documents with confidential/personal data unattended and who can see it or may take it.
- Adhere to data security protocols in public spaces, for example on a flight or a train.

Access Controls

Access Controls ensure our colleagues are given limited access to sensitive data based on the Michael Lonsdale Group's business needs.

This also forms part of the Onboarding and Offboarding procedures which describe the process when a colleague starts or leaves the Michael Lonsdale Group.

The process to grant access rights to the Michael Lonsdale Group network requires:

- Issuing each user, a unique user account/ID (where required); and
- Grant permission to access folders and sensitive data access based on the colleagues and/or third-party contractor’s business purpose and role (for example admin/general user).

- Subcontractors are not given access to business systems and are only given access to collaboration tools and in some cases limited access, including Kiosk Mode on tablet devices, for remedial identification purposes.

Please refer to the **Access Controls Policy** for more information.

Procurement of Devices and Software

For non-standard software requests, the requests must go via the DHTS ticketing system which will validate requests with the Michael Lonsdale Group.

Additional hardware requisitions will also be routed through DHTS via the New Equipment Process, with confirmation from Michael Lonsdale Group senior management required for approval.

High-value requests will be approved or declined by Senior Management.

A central user log is maintained between DHTS and the Michael Lonsdale Group.

Onboarding/Offboarding Procedure

The enrolment process for hardware and login provisioning to employees is managed by the new staff member or subcontractor completing an induction document and the relevant details being submitted to DHTS system provisioning.

Currently, roles are assigned to users and maintained manually by DHTS.

For leavers, the same procedure is followed whereby the access rights are removed and the data erased, with hardware collected by the business and reissued.

User accounts are monitored by DHTS.

Staff and Subcontractors are also required to agree to suitable Information Security contract clauses.

The following steps are to be taken for all members of staff.

Joiners

- Access controls are defined and logged.
- Multiple factor authentication (if possible) and initial password setup.
- Inventory of any assets given to the individual logged.
- Software installed and licenses logged.
- Security Training and Policy Access.

- HR documents updated.
- Entry access fobs are provided.

Movers

- Review of access controls and enhancement/downgrading carried out.
- Review of hardware and physical access.
- Review of software licenses and appropriate addition or removal.

Leavers

- Assessment and immediate removal of access to data at the point of notice being handed in. This is managed on a case-by-case basis.
- All system access is removed on leaving.
- Access fobs returned and/or deactivated (if relevant).
- Hardware checked for data, once backed up if deemed useful, device wiped and recycled into the Michael Lonsdale Group.
- Leaving date and time logged.

Hardware

Devices

All personal device usage must have permission from a Line Manager otherwise devices are provisioned following our Onboarding/Offboarding procedure.

As we operate within on-premises and cloud-based IT systems, supported by Microsoft Intune and Multi-Factor Authentication, staff can use their own devices (BYOD) when necessary, however these must meet all Michael Lonsdale Group (IT) requirements and software controls facilitated by the company deploying its Microsoft Intune and Microsoft App protection software.

MICHAEL LONSDALE GROUP

Mobile Devices and Acceptable Use

Employees using a company or their own devices (BYOD) to perform business tasks (such as reading and responding to emails) must ensure that:

- The devices are secured with suitable passwords, passkeys, PIN's or at least biometric (fingerprint/facial recognition) access.
- Devices must be kept up to date with the latest mobile operating system releases (Android/iOS etc).
- They do not use rooted or jailbroken devices to access services.
- They do not load pirated or illegal software onto devices that are intended to be used for work purposes.
- Due care is taken when sending emails from personal devices that personal and work emails are not confused or merged.
- All personal devices needs to conform to the same security requirements as if it were a corporate device. This includes the account being used on the PC not being an Administrator account (This doesn't prevent the user from not having administrator account details for their personal device, just that the main account used daily is not administrator).
- Personal devices should have antivirus software installed, enabled and up to date.

Remote and On-Site Working

The following controls must be adhered to by individuals working remotely using any type of device:

- If using their own device(s), employees do not download any company or third-party information onto the device's hard drive or removable media. If required for part of a task, then the data must be fully deleted immediately after use.
- They do not use open/unsecured Wi-Fi locations or hotspots when accessing company information.
- They do not leave devices, especially unlocked, in public places.
- They do not share login credentials or other access information with other individuals from within or without the company.
- They use the same due care and attention to opening email attachments and downloading data that they do with home and work computers.

- When being transported, mobile devices as well as being locked/password protected should always be within sight of the employee or on their person and never left unattended.

- They will not transfer any client data to the device or external devices.

- Remote working should be limited to home or a known secure location.

Hardware Protection

The Michael Lonsdale Group laptops are managed by DHTS and comprise of:

- Endpoint security software (antivirus) is installed on all devices.

- Firewalls
  - Enterprise network firewalls at all office locations.
  - Built-in device firewall controls are always on.

- Network and Wi-Fi
  - Segregated Wi-Fi for guest access.
  - DHTS manage all LAN/WAN management and configuration.

- User accounts
  - All users are set up with limited accounts by DHTS (No admin access).

- VPN
  - Windows SSTP VPN to access legacy systems and obtain network licenses remotely.

Patching

Default auto-updates for security patches are set by DHTS and users are shown how to ensure updates are applied and follow on-screen instructions. All updates (operating system and third-party software) must be installed within 14 days of becoming available. DHTS via its management tools will enforce these updates via a patch management schedule. Personal devices (BYOD) should also comply with this 14-day update window however personal devices are not managed by the company or DHTS. It is the responsibility of the user to make sure personal devices accessing company data are kept up to date.

End-of-life (EoL) hardware is disposed of and replaced, with regular checking on the compatibility of current hardware/monitoring of EoL devices.

DHTS and the Workplace Lead also provide a support function to employees for any questions on updates.

Asset Register

The Michael Lonsdale Group currently maintains an asset register which is managed between DHTS and the Michael Lonsdale Group through a Remote Monitoring Management agent and is updated with changes to hardware throughout the organisation.

Remote Wiping and Access Controls

DHTS can lock and remove access to any devices connected to our domain pool and track those that are connected to the internet as well as wipe devices that are connected to the Michael Lonsdale Group Mobile Data Management System or Intune.

USB and Other Devices

Employees must not plugin or use non-approved (not purchased by the Michael Lonsdale Group) mass storage devices such as USB sticks and external drives to the Michael Lonsdale Group hardware systems without prior agreement from a Line Manager or other senior staff member.

Safe Disposal of Devices

DHTS is responsible for End of Life disposal of hardware which includes wiping and secure destruction, or if the devices are to be recycled back into the Michael Lonsdale Group or returned to a leasing company or any other action, resetting to factory settings and ensuring data artefacts are not present.

Software

All software on the Michael Lonsdale Group devices is preinstalled, with requests for new software managed through the process detailed in the procurement of devices and software.

All hardware is locked to non-Admin access so the Michael Lonsdale Group employees cannot download and install software themselves.

Installation of software by DHTS is only from official download locations and systems are scanned on the installation of any additional software that follows the above process.

Refer to the approved software policy for a full list of the approved software within the group.

Testing

All systems are tested frequently by DHTS, including ensuring security patches are up to date, checking EoL devices, running network scans and checking defender logs.

Data

Senior staff should be aware of the retention periods on data and perform regular audits on network/server stored data and its relevance. Digital data destruction must also be performed as part of a Subject Access Request if requested.

When removing data, it is essential that the items are removed from any syncing operations (for example storage in a cloud provider such as Microsoft 365), emails and the recycle bin on the PC or server.

Data In Transit and At Rest

All data at rest is encrypted and client-server communication in transit is encrypted.

HTTPS is used by default when using browser-based applications.

All email traffic uses standard TLS encryption.

Data Back-Ups

Business-critical back-ups are managed using cloud-based Microsoft Office 365. All backups are managed by DHTS and are done in real-time.

Password Management

DHTS ensures to the best of its abilities:

- It enforces strong passwords for user set-up.
- It requires changes to first-time passwords.
- It forces the expiration of first-time passwords.
- It enforces the strictest controls for system-level access.
- It enforces all the password policy controls applicable to users for administrative functions.
- Two Factor Authentication/Multi-Factor Authentication (2FA) is in place where appropriate.

Password Training

Users are instructed on:

- Not sharing passwords with others or writing them down.
- Using a passphrase which is a sequence of words and numbers rather than dictionary words.
- Avoid reuse of passwords for different systems/websites.
- Never asking others for their passwords.
- Never using restricted data such as birth dates for passwords.

Two Factor/Multi Factor Authentication

Where possible, and if the software permits, the Michael Lonsdale Group's default policy is to apply 2FA to devices and software.

MICHAEL LONSDALE GROUP

Acceptable Use

General Policy Points

- All individuals working at or for the Michael Lonsdale Group are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be away from their workstation for even short periods.

- Computer workstations must be locked when a workspace is unoccupied.

- Any Restricted or Sensitive information must be removed from desks and locked in a drawer when the desk is unoccupied – even for short periods and at the end of the workday.

- Filing cabinets containing sensitive information must be kept closed and locked when not in use or when not attended to and when staff members are expected to be absent for even short periods.

- Computer screens must be locked when unattended.

- Passwords must not be written down.

- Printouts containing sensitive information should be immediately removed from the printer.

- Upon disposal, sensitive documents must be shredded.

- Whiteboards containing sensitive information must be erased immediately after use.

- Mass storage devices such as CDROM, DVD or USB drives must be treated as sensitive and therefore must be secured in a locked drawer when not in use.

- All printers and fax machines should be cleared of papers as soon as they are printed.

Physical Data/Clear Desk

When paper copies of information are needed, they should always be destroyed after use.

Staff should also take responsibility for clearing out any old documentation - even if it is not their own.

For example, notebooks and other artefacts that others have left behind. If they are not needed anymore and locked away, they should be placed in a shredding machine.

Other examples of documents that should be destroyed:

- Meeting notes.
- Client design, notes and diagrams.

Desks should be document free when not in use, with any printouts stored in locked drawers when a member of staff is not present.

Working Remotely

- When home or remote working due security care and attention should be paid, including securing devices and laptops, particularly when being left unattended.
- Devices or laptops must not be left in a vulnerable position, for example in public view.
- Devices that are logged in to the Michael Lonsdale Group services should not be shared with or accessible to other members of the household or other parties.
- A clear desk policy should still apply when away from an office location.
- Due care and attention should be paid to surroundings.
- In public spaces, eavesdropping should be considered before making any client or company-sensitive calls.
- Staff must not use open/unsecured Wi-Fi locations or hotspots when accessing the Michael Lonsdale Group information or systems.

Lost or Stolen Devices

Any lost or stolen devices must be immediately reported to a Line Manager or DHTS.

Acceptable Use and Monitoring

Various monitoring, recording, filtering, and other similar applications are used to maintain the integrity of the Michael Lonsdale Group systems and network. For example:

- To identify or prevent inappropriate use of the Michael Lonsdale Group's email, internet, and other information systems.
- To prevent the introduction of viruses and other external threats.
- To ensure that system performance is not affected by personal use.
- To establish the details of transactions or other matters relevant to the business of the Michael Lonsdale Group.
- To respond to a court order or a discovery request in relation to legal action.
- To prevent or detect crime or serious breaches of the company's corporate policies.
- To ensure compliance with regulatory or self-regulatory practices and procedures relevant to the business of the Michael Lonsdale Group.
- To provide information relevant to legal proceedings, subject access, or freedom of information requests.

Please refer to the Michael Lonsdale Group Email, Internet, and Communications Policy for more details.

Physical Security

Physical office locations:

- Will have a secure entrance that is manned and if not manned then the appropriate areas are locked.
- Staff will challenge anybody who they are not familiar with that they encounter in the building.
- Staff will ensure that no person or persons 'tailgate' them into the secure area when gaining entry via an access fob or other controlled door.
- Offices are locked if not being used and access will be through access fobs.
- All offices have 24/7 motion sensors and appropriate notification systems where possible.

- Staff are aware of the procedure for notifying the receptionist if they lose or have their access fob stolen and this will be deactivated immediately.
- Any visitors are logged with their validated identity and time/date by the receptionist.
- The Clean Desk Policy is adhered to, and desks are checked at regular intervals.
- Physical documents are either locked away or shredded if not needed – no matter what the content of the documents.
- Laptops are locked when absent from the location.

IT Security Incidents

Breach and Attack Procedure

The Michael Lonsdale Group uses the following 5 step procedure for attacks, breaches, and other IT-related issues:

Step 1: Identification and Initial Assessment.

Step 2: Immediate Containment and Recovery.

Step 3: Risk Assessment and Investigation.

Step 4: Notification.

Step 5: Evaluation and Response.

Identification and Assessment

Any person who uses or accesses the Michael Lonsdale Group or the Michael Lonsdale Group Client data and work products is responsible for reporting a breach or other information security incidents immediately to a Senior Manager and the Data Protection Officer (DPO).

Breaches or suspected breaches must be reported as soon as possible and contain all the information known about the suspected or verified incident.

For initial reporting the information below should be communicated to the relevant individuals internally:

- If the breach is confirmed.
- The actual data involved in the breach.
- The cause of the breach.
- The nature of the data involved in the breach.
- The number of records involved in the breach.
- Containment recommendations.
- The actions that have already been taken to contain the breach.

Containment and Recovery

Containment and Recovery is the procedure that is actioned if it is determined that anything can be done about the breach right away.

For example, if a physical theft has taken place this would be recovery actions, or if a cyber breach the restoration of data, disaster recovery, further encrypting data, changing VPN/network tunnels and/or changing passwords.

Because of the varying nature of potential breaches, the containment and recovery actions that are required will need to be determined by Senior Managers. Where Client data is the subject of the breach this will also include the Client DPO and any additional sub-contractors or 3rd-parties involved in the breach.

Risk Assessment and Investigation

At this stage, the Michael Lonsdale Group performs a Risk Assessment which will lead to an incident report considering the following:

- The types of data involved.
- The sensitivity of the breached data.
- Protection and containment actions that have already been undertaken.
- Any further information that is known about the breach and its intentions.
- Volume and risk of personal or company data breached for the Michael Lonsdale Group or the Michael Lonsdale Group clients.
- Risk to companies and organisations from the breach.
- Financial implications to individuals and organisations.
- Any further risk to involved parties such as legal, reputation and continuity of services.

Incident Log

All incidents will be logged in a Breach Incident Log that is visible to Head Office.

Notifications

After the Risk Assessment is complete, the Michael Lonsdale Group will determine if the breach or another issue warrants notifications to individuals, police, assessment and compliance bodies or any other groups.

Response

For breaches that are classed as severe the local technical team, with support from other business units or Head Office if required, will perform a full evaluation based on the incident report and any required 3rd party data collection. This will contain:

What has been done and will be done to reduce the risk of the same type of breach in the future?

- Do any more security controls need to be implemented to reduce the risk?
- Was the breach due to staff training and does this need improving?
- Was the breach due to a 3rd party service and does this relationship need reviewing?
- Are there any other measures that can be taken to mitigate risk?
- Recommendations for process and procedure updates.

Please refer to the **Incident Management Policy** for more information.

Policy Access

This policy is available internally to all staff through the network and provided as part of onboarding and regular training updates.

DHTS Helpdesk Contact Details

support@dhts.co.uk

+44 (0) 20 3475 5699

Potential Sanctions

All deliberate breaches of this policy will be investigated under the Disciplinary Policy.

Users who do so will be subject to disciplinary action, up to and including termination of employment or service contract.

Breaches will be escalated to the Board of Directors as part of the organisation's risk management process and reviewed.

Employees, contractors, and other users may also be held personally liable for violating this policy.

Where appropriate, the Michael Lonsdale Group will involve the police or other law enforcement agencies concerning breaches of this policy.

Monitoring and Reviewing

This policy will be reviewed and updated yearly or when significant internal changes (such as system upgrades) occur.

Name: G Herbert For and on behalf of the Michael Lonsdale Group

Position: Managing Director

Signature: 

Date: 9th September 2022