Access Controls Policy

Introduction

This Access Control Policy (ACP) for 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) covers employee and subcontractor access to the Michael Lonsdale Group and client systems as well as further information concerning security controls around day-to-day operations.

The purpose of this document is to detail the Michael Lonsdale Group's policies and procedures for giving users access to systems and data in the course of their day-to-day work. Providing these controls ensures any security risks are minimised and users only have access to systems that are required to fulfil their role.

Scope

This policy applies to the directors, employees (full-time, part-time or casual), volunteers and subcontractors of the Michael Lonsdale Group.

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

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

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

We will review and update this policy adhering to our data protection obligations. It does not form part of any employee's contract of employment, and we may amend, update, or supplement it from time to time.

We will circulate any new or modified policy to employees and any other stakeholders when it is adopted.

Responsibilities

All users have the responsibility for protecting the data and information that they manage or access from corruption, deletion or dissemination.

Usage of information systems and being granted access to the Michael Lonsdale Group data indicates acceptance of and compliance with this policy.

Users will be provided training and any other assistance they may require ensuring they understand both the systems in place and the Access Control Policy.

Core ACP Controls

- User Access Rights are managed by the third-party Managed Services Provider (MSP) D H Technical Services Limited (DHTS)
    - Requests for increased access should follow a standard change request procedure from the user to the Michael Lonsdale Group management with a case for usage rights required.
    - Internal IT teams manage the technical configuration and setting of access privileges for software at all times.
- Any known or suspected data breaches should be reported in line with the Michael Lonsdale Incident Management Policy.
- Employees and subcontractors will only access personal and sensitive personal data as well as business data in line with specific requirements of their role (Principle of Least Privilege).
- Passwords, where possible, will be controlled through the central password management system and must be strong, complex and supported by multi-factor authentication (MFA).
    - Staff are trained in password management, including not reusing passwords, never asking others for their passwords and not sharing or writing passwords down.
- If there is an option, software should always be configured using MFA. However, users must not use their own non-company devices for MFA which could lead to a lack of access or restriction of data access that the company may require.
- Users must never access third-party (for example, clients) data without prior authorisation and as part of their role at that specific time. For example, if access is required for a task, this does not mean access is still granted after that task has been completed.
    - If users can access a data store, for example in SharePoint, that contains personal information, they should not do so for browsing, unless it is specifically related to a company task.
- Employees are required to read our client's policies and procedures for information security and access before being granted access to their systems.

- Third-party access must never be granted to any of the Michael Lonsdale Group data without a director's written consent or to client data without their prior written consent and defined objective.

Third-Party Security

The Michael Lonsdale Group will ensure any employed subcontractors:

- Are contracted to adhere to the Michael Lonsdale Group and standard Data Protection and Information Security guidelines.
- A Non-disclosure agreement should be signed to protect company data and information.
- Have enough technical insurance in place.
- Have a verified and implemented security policy which will be reviewed by the Michael Lonsdale Group.
- Will conform to the Michael Lonsdale Group policies and procedures including breach reporting.
- Will enter, where relevant, into written supplier-subcontractor agreements determining the use of sub-processing of any business or personal data and make the affected parties aware of any agreements.
- Undertake any Michael Lonsdale Group cyber threat training and read our company policies and procedures.

Access Controls

Access Controls ensure our colleagues are given limited access to 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 new colleague starts and leaves the company.

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

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

Principle of Least Privilege

System access is managed using the Principle of Least Privilege – users only have access to data and systems they need to complete their role at the Michael Lonsdale Group.

Currently, Active Directory is segregated into:

- Non-Administrator user roles
- Basic Administrator access.

All security devices are configured at an Administration level with:

- Endpoint Security software
- Microsoft Intune.

Onboarding/Offboarding Procedure

The enrolment process for hardware and login provisioning to employees is managed by DHTS.

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

- All staff are required to read our policy and procedure documentation at the start of their role
- All leavers must have their credentials removed immediately and their devices wiped on their date of leaving.
- Subcontractors are also required to agree to suitable contract clauses.

Monitoring

All Michael Lonsdale Group systems have system logging, with elevated permissions able to check users current and previous activity if required.

- User accounts are monitored by DHTS and Senior Management/Decision Makers.
- Active Directory administration changes are logged and auditable.

Networking Controls and Change RequestS

All networking at the Michael Lonsdale Group offices is managed by DHTS.

No third party/own devices are permitted to attach to the company or client's network without prior approval from Senior Management/Decision Makers.

Please refer to our **Mobile Devices Policy** for more information.

Change Control Procedure

Any changes to network/system configuration are done through an internal change control process detailing the request, approver and risks. In the majority of cases, a fallback plan for reverting to previous system implementation will be detailed and in place.

If a change is approved at the Senior Management/Decision Makers level the modifications must be quality assured in a test environment before implementation.

Endpoint Protection

All offices have enterprise class firewall protection device is in use and managed by DHTS.

MICHAEL LONSDALE GROUP

Clear Desks

The below policy points are the minimum requirements for the Michael Lonsdale Group management of confidential or sensitive information and the access to it by other colleagues or guests.

- 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 desk for even short periods.
- Computer workstations must be locked when a workspace is unoccupied.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied even for short periods; and at the end of the workday.
- Filing cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended to and when the staff members are expected to be absent for even short periods.
- Passwords must not be written down and left in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- When no longer required, Restricted and/or Sensitive documents should be shredded.
- Whiteboards containing Restricted and/or Sensitive information should 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 should be cleared of papers as soon as they are printed.

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

Position: Managing Director

Signature: 

Date: 9th September 2022

MICHAEL LONSDALE
GROUP