Incident Management Policy

Introduction

This document outlines 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) management and processes to follow for various IT-related incidents. These procedures cover minor technical enquiries to full breaches and disruptions to business as usual and ensure:

- Incidents are managed in a consistent way to protect our clients and the Michael Lonsdale Group.
- Business as usual is restored for any parties affected as soon as possible for all affected parties.
- Root causes analysis and subsequent Corrective and Preventative actions take place for all incidents.
- Incidents are logged and communicated to affected parties adhering to the law.

Scope

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

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.

Incident Type Definitions

The following incident types are relevant:

Non-Security Incident and Support Definitions

General IT Support Enquiries

- System questions.
- Training and instructions.

Hardware

- Gaps in user knowledge on device usage.
- Damaged devices.
- Lost devices.

Software

- Bugs in software.
- Loss of functionality.
- Inability to access domains/files.
- Lockout.

MICHAEL LONSDALE GROUP

Security Breach Incident Definitions

- Data Breaches
- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.
- Compromised User Accounts.

Further examples of Data Breaches are:

- Verbal Disclosure: Sharing private information.
- Insecure Disposal: Not destroying data in its entirety.

Cyber Attacks

- Malware: Embedded software that gathers or leads to the gathering of data.
- Phishing: Emails or other means that trick the end-user into believing a website or other asset has legitimate interests whereas it captures data for illegal activities.
- Password Attacks: The attacker uses a script to guess many combinations of passwords leading to data access.
- Ransomware: Malware installed that demands a ransom for encryption.
- Denial of Service: The attacker uses a script to flood the target with requests, leading to its crash with potential data theft.
- Unauthorised Access: Access from individuals not legally allowed to access data.
- Social Engineering: Users giving away information that leads to data breaches to individuals they believe represent a legitimate interest through confidence tricks.

Non-Security Incident Actions and Expected Outcomes

Non-Security incidents will be dealt with by the third-party Managed Services Provider (MSP) D H Technical Services Limited (DHTS).

The end-user will:

- Communicate the issue through telephone or email to the DHTS helpdesk.

DHTS will:

- Log the issue.
- Identify the issue.
- Categorise the issue.
- Prioritise the issue.
- Assign the issue; or
  - Escalate the issue.
- Diagnose the issue.
- Resolve the issue; and
  - Seek departmental authorisation if budget sign-off/other uplift is required.
- Communicate and log the issue.
- Close the issue.
- Feedback on any learnings from the issue(s) into IT Team meetings if mitigation of future similar occurrences is possible or if commonalities are found in several issues.

If the issue involves a lost device, it must also be considered a potential security breach incident – especially if the device contains easily accessible personal or business-sensitive information.

Security Breach Incident Reporting and Expected Outcomes

Please refer to the section **Security Breach Incident Definitions** for examples of security breaches.

Responsibilities

- All those who handle or process the Michael Lonsdale Group information must be familiar with this procedure and comply with its terms.

- All those who handle or process the Michael Lonsdale Group information are responsible for reporting any data protection breach or information security incident under the terms of this procedure.

The Michael Lonsdale Group Data Breach Procedure

Below are the 5 steps to managing a Data Breach that the Michael Lonsdale Group uses:

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.

Breach Types

1	2	3	4	5
No significant reflection on any individual or body. Media interest very unlikely	Damage to an individual or company's reputation. Possible media interest, e.g. high-profile individual(s) involved	Damage to the Michael Lonsdale Group/ clients reputation. Some local interest that may not go public/ Low key local media coverage.	Damage to an organisation's reputation/ Local media coverage.	Damage to the Michael Lonsdale Group or clients reputation/ National media coverage.
A minor breach of confidentiality. Only a single individual affected	Potentially serious breach. Less than 5 people/records affected, or risk assessed as low, e.g. files were encrypted	Serious potential breach & risk assessed high e.g. unencrypted sensitive business records lost. Up to 100 people/records affected	A serious breach with either sensitivity e.g. sensitive business or personal details, or up to 1000 people affected	A serious breach with either sensitivity e.g. sensitive business or personal details 1000+ people affected

Identification and Assessment

Any person who uses or accesses the Michael Lonsdale Group data is responsible for reporting a breach and other information security incidents immediately to a Senior Manager and the IT Team.

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 data involved in the breach.
- The cause of the breach – please refer to Breach Types above.
- 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.

After the initial reporting of the incident, the Michael Lonsdale Group team members with support from DHTS will perform an assessment and undertake an investigation that follows the sequence of events below.

There is no standard scale to measure data breaches currently. The initial assessment will determine the scale of the breach based on the Breach Types table.

Containment and Recovery

Containment and Recovery is the procedure that is actioned if it is determined if 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 tunnels and/or changing passwords.

Because of the varying nature of potential breaches, the containment and recovery actions that are required must be determined by the IT team with support from the Technical Director or an external service provider if necessary.

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 data breached.
- 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.

Notifications

After the Risk Assessment is complete, the Michael Lonsdale Group will determine if the breach or other issue warrants notifications to the following:

- The Michael Lonsdale Group clients.
- The Crown Commercial Services if the client was procured through a Government Commercial Marketplace (UK).
- Local Police or Security Services.
- The Information Commissioner's Office (UK).
- Insurance Companies.
- Legal Consultants.
- Data Subjects and organisations affected by the breach.
- Any other relevant parties.

All “notifiable” breaches must be reported to the ICO within 72 hours of The Michael Lonsdale Group becoming aware of the breach.

- Any breaches involving the loss of personal data must always be reported to the ICO (UK).
- Any breaches of a controller’s data must be reported to the controller within 72 hours.

From Article 32 of UK GDPR.

“ In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.”

Example of a notifiable breach

An example of loss of personal data can include where a device containing a copy of a client's customer database has been lost or stolen.

A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware or has been encrypted by the controller using a key that is no longer in its possession. This is a notifiable breach.

Example of a non-notifiable breach

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device utilised by the controller and its staff.

Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker.

This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects or organisations in question.

If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

If in doubt, the Michael Lonsdale Group will contact the ICO. The most up-to-date contact information and reporting procedures can be found on their website:

https://ico.org.uk/for-organisations/report-a-breach/

Information to have ready for reporting a data breach:

- Your name and contact details.
- The date of the breach.
- A summary of the incident.
- The likely effect on the data subjects.
- Any measures you have taken to address the breach; and
- Any steps the data subjects can take to protect themselves from harm.

MICHAEL LONSDALE GROUP

Evaluation and Response

For breaches that are classed as severe (over 100 records breached with personal or sensitive business information) the IT Team, with support from The Michael Lonsdale Group Directors 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.

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

Position: Managing Director

Signature: 

Date: 9th September 2022