Title	Information Security Incident Policy
Process Owner	MD + HSEC
Date Created	16/06/2020
Publish Date	03/10/2022
Approved By	Management Team
Summary	Policy detailing how security incidents are categorised, the reporting mechanisms and the actions to be taken should an event occur.
Classification	Public
Standard	IS
Version	4.0

Change Record
Enter any changes to the document within the tag below…
Updates based on ADISA requirements – addition of reference to severity, addition of data breach notification and addition of reporting within Improvement Forms.
Overwrite the content of the tag, this will create each change you have made to the document and record it in ISOportal

Information Security Incident Policy

Introduction

In order to effectively maintain the confidentiality, integrity and availability of information assets within Middleton Asset Management Identified security incidents are to be investigated using the Security Incident Investigation Report. All Security incidents are to be handled in a timely and effective manner.

The purpose of this policy is to ensure the identification, investigation, resolution and response plan of security incidents, minimising their business impact and reducing the risk of similar security incidents occurring. This policy shall ensure the implementation of appropriate security incident management measures to minimise the risk of:

- Information being corrupted, destroyed, stolen and/or lost
- Computer performance being disrupted and/or degraded
- Financial and reputational loss
- Productivity losses being incurred.

Responsibility

- All members of staff are always to remain vigilante, to reduce the potential of a security incident occurring in the first place.
- You are responsible for reporting “near-miss” (or potential) incidents to the relevant person.
- You are responsible for reporting an actual security incident to the relevant person.
- You are responsible for not being the source of the information security incident by following the guidance given in all our policies within our Management System.

Detail

- We have identified the following resources that could be the target of and/or the source of a security incident: -
  - network devices
  - servers
  - computers/laptops
  - applications
  - databases
  - operating systems
  - printers
  - email
  - internet access
  - physical access

- members of staff
- visitors

- All security incidents are to be recorded on the Improvement form (if considered minor in nature) or on the Helpdesk System for further investigation and/or escalation. These are retained for a minimum of 3 years on the system.
- All members of staff will report all security incidents to their manager in the first instance or to the IT provider.
- If a security incident is declared to be a Data Breach, then the ICO (https://ico.org.uk/) are to be informed within 72 hours as per the Data Protection Policy.

What is an Information Security Incident?

- The definition of a security incident is defined as a breach of policy or an adverse event that has led or could lead to a compromise of information or a device owned or processed by Middleton Asset Management .
- Severity of security incidents are assigned as per the Improvement Process.
- Severity levels are a measurement of the impact an incident has on the business. Typically, the lower the severity number, the more impactful the incident. The diagram below defines Asset Disposals severity levels

Severity level	Description	Examples
1	A major incident with very high impact	A customer-facing service, like data security is compromised. Confidentiality or privacy is breached. Customer data loss.
2	A minor incident with medium to low impact	A minor inconvenience to customers, workaround available Usable performance degradation
3	A opportunity for improvement, an incident with very low impact	Little to no impact on our customer. Improvements identified with AD's process

- All information security incidents are to be reported immediately to our IT provider.
- Information security incidents can be accidental or malicious.
- Examples of information security incidents are:
  - unauthorised access to information;
  - unauthorised modification of information;
  - unauthorised disclosure of information;
  - action that leads to unauthorised denial of service to information;
  - loss or theft of assets containing information;
  - failure to protect information in line with our Information Security Policies on ISOportal;

- malicious or careless employees;
- malware (computer viruses, worms, Trojan horses, most rootkits, spyware and other malicious and unwanted software);
- social engineering;
- spam;
- spoofing and phishing;
- man-in-the-middle attacks;

This list is not exhaustive.

What is a Physical Security Incident?

- A Physical security incident are defined as a physical action has taken place to compromise our premises
- All physical security incidents are to be reported to the designated personnel for the security of our premises and facilities
- Examples of a physical security incident: -
  - Break-in to our premises or vehicles
  - Theft of equipment
  - Doors left unlocked (internal and external), where they are designated to remain in a locked state
  - Security alarm not being set
  - Criminal damage
  - Unauthorised access to secure areas
  - Tailgating - allowing unknown people to follow you through security barriers
  - Loss of or stolen company ID badge

This list is not exhaustive

Data Breach Notification

All Personal Data breaches must be reported immediately to the HSE & Compliance Manager and must be added to the register of Personal Data breaches (Improvement Forms).

Middleton Asset Management as a Data Processor

Where Middleton Asset Management is a Data Processor, and a Personal Data breach occurs, and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Controller must be notified immediately with further information about the breach provided as soon as information becomes available.

Middleton Asset Management as a Data Controller

Where Middleton Asset Management is the Data Controller, unless a Personal Data breach occurs which is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the relevant supervisory authority must be notified of the breach without delay, and in any event, within 72 hours after having become aware of it, if this is feasible. If the notification is not made within 72 hours, it should be made as soon as possible, together with reasons for the delay. The Information Commissioner's Office (ICO) is the supervisory authority in the UK

In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of Data Subjects, all affected Data Subjects are to be informed of the breach directly and without undue delay.

Irrespective of whether Middleton Asset Management is a Data Processor or a Data Controller, all data breach notifications must be handled strictly in accordance with the Middleton Asset Management Personal Data Breach Procedure and be added to the Middleton Asset Management Personal Data Breach Register (Improvement Forms) which are located ISO Portal.

Information Security Incident Response

- Upon the reporting of a security incident the person responsible will begin the process of recording the details in the Improvement Form
- If the incident is deemed to be severe in nature, which could cause irreparable harm to our facilities or reputation then the Business Continuity Plan will be enacted and followed; this will be recorded on a BC Report.
- If the reported incident can be handled in the normal operational activities, then the following tasks will be undertaken: -
  - Investigation of the source of the incident
  - Decision by the competent personnel to either switch off or disable the affected device or service, or to quarantine the affected device for further investigation of the source
  - Removal of any malicious software or application that is causing the problem
  - A rebuild of a device, if required to ensure no lasting effects
  - Reporting to the authorities in a timely manner if required
  - Incident response disclosure plan to customer including corrective action and root cause report.
  - Training and instruction given to the affected party on how to prevent a re-occurrence of the incident
  - Recording all actions taken and lessons learned from the incident
  - Informing Top Management that a security incident has occurred
- Capture of evidence will be decided by the Management Team based on nature of event; a high level of detail will be added to the Improvement Form referencing where all evidence can be located.
- Investigation Report will be held on the Improvement Form including root cause analysis.

Security Incident Response for DIAL 3 Customer

- Upon receipt of any DIAL 3 data at the unit any loose or separate data carrying product or media including tape which are not listed on the inventory shall be quarantined and raised as an incident and investigated. The warehouse team are to conduct the following:
  - Inform the Operation Manager and HSEC Director immediately
  - Operation Manager is to inform the Account Manager
  - HSEC to start incident and investigation process following the Security Investigation Report
  - Warehouse team to place the whole consignment into quarantine.
  - Account Manager is to inform the client and await direction
  - Account manager to is inform all of clients requirements.
  - HSEC on completion of the investigation is to raise improvements and report as required

Near Miss Response

- A near-miss is where you have taken action to prevent an incident occurring
- This can be: -
  - Closing and/or locking a door that was left opened or unlocked
  - Locking a device that had been left logged on
  - Putting a device, hardcopy information in a secure location, where it should have been
  - Removing information from a printer and giving it to the owner
  - Reporting suspicious activity on site
  - Witnessing someone escalating their permissions on any system (this can be considered an actual event)

This list is not exhaustive

- Your actions to safeguard our facilities should be reported to the Management Representative