Southern Lightning Engineers Limited
Unit D2/1, Bearsted Green Business Centre, The Green, Bearsted, Maidstone, Kent. ME14 4DF

Information Security Incident Management Policy

Issue Date: 09 July 2018

1 Policy Statement

Southern Lightning Engineers Limited will ensure that it manages appropriately any actual or suspected incidents relating to information systems and information within the custody of the organisation.

2 Purpose

The aim of this policy is to ensure that Southern Lightning Engineers Limited manages appropriately any actual or suspected security incidents relating to information systems and data.

3 Scope

This document applies to all Employees of the organisation.

All users **must** understand and adopt this policy and are responsible for ensuring the safety and security of the organisations systems and the information that they use or manipulate. This includes both data stored electronically and in any other form.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

4 Definition

This policy needs to be applied as soon as information systems or data are suspected to be or are actually affected by an adverse event which is likely to lead to a security incident.

The definition of an “information management security incident” (‘Information Security Incident’ in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation’s assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the organisations knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 2.

5 Risks

Southern Lightning Engineers Limited recognises that there are risks associated with users accessing and handling information in order to conduct business.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up consistently and correctly.
- To help identify and deal with areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

6 Procedure for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the organisation. It is vital for the organisations ICT Department to gain as much information as possible from the business users to identify if an incident has taken place or is occurring.

For full details of the procedure for incident handling please refer to Appendix 3.

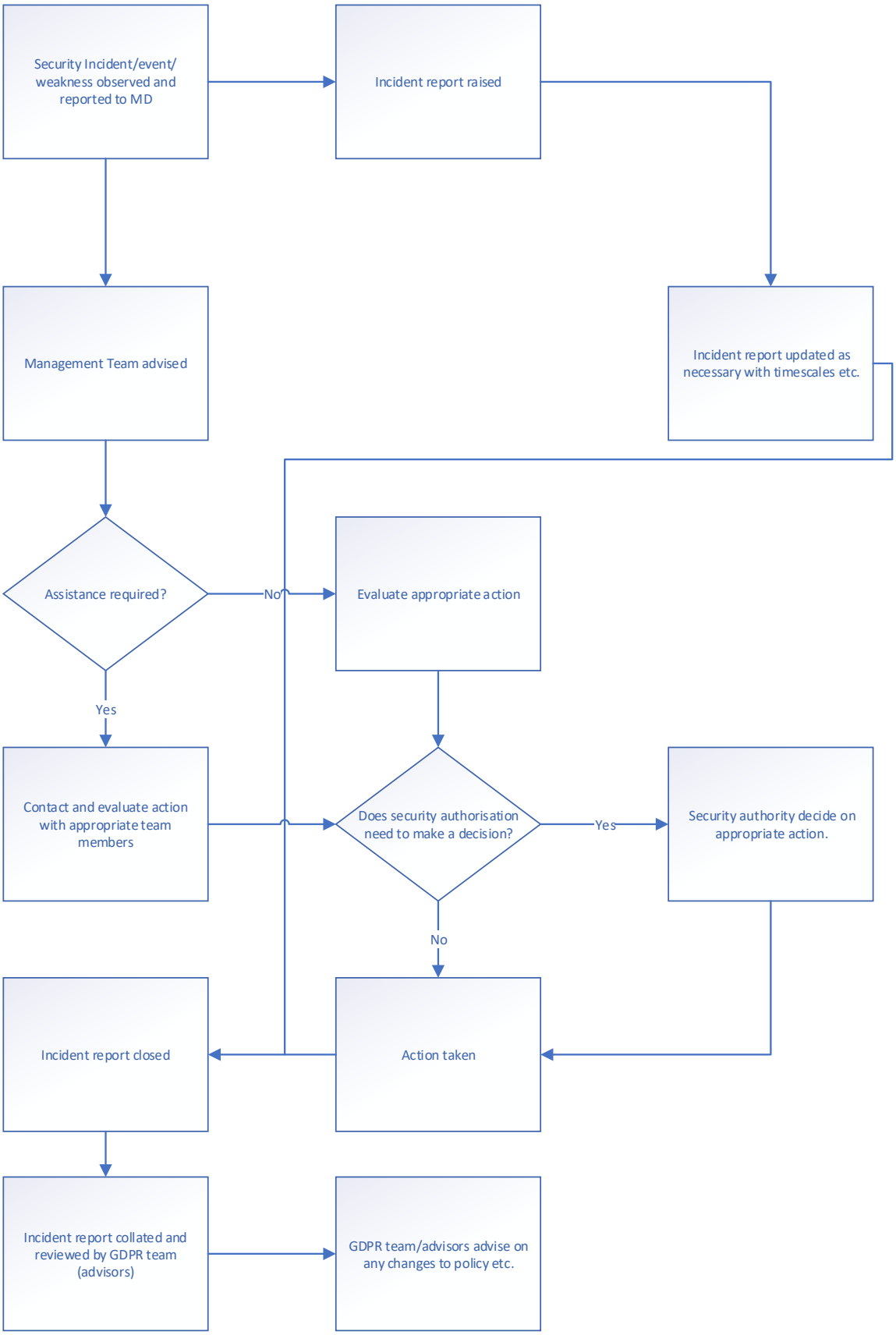
7 Policy Compliance

This policy applies to all employees. If any user is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

8 Review and Revision

This policy, and all related appendices, will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

9 Appendix 1 – Process Flow; Reporting an Information Security Event or Weakness


Security Incident/event/ weakness observed and reported to MD
Incident report raised
Management Team advised
Incident report updated as necessary with timescales etc.
Assistance required?
No
Evaluate appropriate action
Yes
Contact and evaluate action with appropriate team members
Does security authorisation need to make a decision?
Yes
Security authority decide on appropriate action.
No
Incident report closed
Action taken
Incident report collated and reviewed by GDPR team (advisors)
GDPR team/advisors advise on any changes to policy etc.

10 Appendix 2 – Examples of Information Security Incidents and Events

Examples of the most common Information Security Incidents and events are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff' by mistake.
- Non-reporting of the receipt of unsolicited mail of an offensive nature.
- Non-reporting of the receipt of unsolicited mail which requires you to enter personal data.
- Changing data that has been done by an unauthorised person.
- Forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others. (Chain letters can be disturbing to those who receive them by implying bad luck if it is not forwarded for example. These are in fact just either at best a piece of fun which clogs up corporate and international email services wasting resource and at worse an attempt to harvest information from the recipient's machine including contacts information, details of corporate firewalls etc. They should be deleted straight away and not forwarded anywhere.)
- Unknown people asking for information which could gain them access to company data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on the organisation's equipment.
- Accessing a computer or database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any of the organisation's computer equipment.

This policy will be enforced through the use of the disciplinary procedure.

Allegations of malicious or misuse will be investigated and action taken in accordance with the disciplinary procedure. The level of action taken in response to any breach will be dependant on the nature and the findings of any investigation of suspected breaches.

Any suspected breaches of this policy will be managed by the local line manager and in accordance with the organisation's disciplinary procedures.

11 Appendix 3 - Procedure for Incident Handling

Reporting Information Security Events or Weaknesses

The following sections detail how users must report information security events or weaknesses. Appendix 1 provides a process flow diagram illustrating the process to be followed when reporting information security events or weaknesses.

Reporting Information Security Events for all Employees

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from IT Staff).
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately.

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Senior Management for the impact to be assessed.

The IT team will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and contact number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Security Events and Weaknesses for IT Support Staff

Security events can include:

- Uncontrolled system changes.
- Access violations – e.g. password sharing.
- Breaches of physical security.
- Non-compliance with policies.
- Systems being hacked or manipulated.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.
- Malfunctions of software applications.
- Human errors.

Learning from Information Security Incidents

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by the organisation and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

Appendix 4 - Incident Report

General Information	
Reported By:	Date/Time Detected:
Department:	Date/Time Reported:
Title:	Mobile:
Phone:	Email Address:
Postal Address:	Additional Information:
Incident Details	
Type of Incident: (Type of data and equipment involved)	
Status of the Department (total failure, business as usual etc):	Classification of affected System:
Incident Details: (Is anyone at risk?)	
Site Details:	Site Point of Contact:
Actions Taken:	