Lesniak Swann
Unfair competitive advantage

Incident Management Procedure

Policy

The Information Security Incident Policy shall be used to produce, implement, test and manage the information security incident procedure for incidents (including IT incidents and suspected data loss/breaches (electronic and physical).

Information Security Incidents

An Information Security Incident is an event, or chain of events, that could compromise the confidentiality, integrity or availability of information. Examples of information security incidents can include but are not limited to:

- Potential and suspected disclosure of client or customer information to unauthorised individuals.
- Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored.
- Disruption to systems and business processes.
- Inappropriate access controls allowing unauthorised use of information.
- Attempts to gain unauthorised access to computer systems, e.g. hacking.
- Records altered or deleted without authorisation by the data 'owner'.
- Virus or other malicious (suspected or actual) security attack on IT equipment systems or networks.
- Human error such as emailing data by mistake.
- Covert or unauthorised recording of meetings and presentations.
- Damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges.
- Deliberate leaking of information.
- Insider fraud.

Information/Data Breach

An information/data breach is a security incident where sensitive, protected or confidential data has intentionally or unintentionally been released or obtained by persons who are not authorized to view or access it.

Information Security Incident Management

Lesniak Swann shall be able to manage incidents affecting clients or customer information assets from identification and analysis, through to response, resolution and recovery.

The Lesniak Swann information security incident management process shall be fully documented to be able to handle different types of information security incident.

Information Security Incident Reporting

Lesniak Swann shall ensure that any incident that could potentially affect the security of information is identified and managed appropriately.

The incident shall be reported to the client via telephone

The process shall be simple, clear and easy to follow. It should follow the below guidelines:

- Use a single point of contact for telephone reporting of incidents
- Following the initial call details of the breach will be emailed and contain the following information:
    - Date
    - Location
    - Short summary of what occurred
    - Type of incident – e.g. e-mail, lost USB device or paper
    - Contact details for obtaining further information

Everyone within Lesniak Swann is responsible for reporting security incidents. All personnel shall be made aware of what constitutes an incident and how to report them.

Information Security Incident Analysis and Response

Lesniak Swann shall ensure that all incidents are assessed as soon as possible, so that the most appropriate course of action and a priority can be given for their resolution. The response to an incident is likely to require the skill and expertise of various groups within Lesniak Swann (IT, operations, legal and human resources) as well as external agencies (police authority, forensic specialists).

The analysis, by the specialists handling the incident, shall include the following processes:

- Assessment of the severity of the incident against client.
- Identification of type of incident – paper loss, e-mail, portable IT media.
- Assessment of scale of incident in terms of data size – e.g. Gb of data or number of pages lost or distribution list.
- Identification of classification or type of data.
- All actions and decisions made during the response to incidents shall be recorded.

Collection of Evidence

Lesniak Swann shall ensure that if an incident is suspected to be caused as a result of a criminal or if legal action is anticipated, then further advice must be obtained from the client and steps taken to ensure that any evidence necessary for a successful prosecution is not intentionally or accidentally destroyed in accordance.

Learning from Incidents

Lesniak Swann shall ensure that all incidents are monitored to establish whether there are any trends that could be addressed. For all major incidents, a post incident investigation of the information security incident and the actions taken to resolve the incident shall be conducted to:

- Determine the root cause of the incident.
- Quantify its impact on client.
- Minimise the possibility of recurrence.
- Improve future responses.
