INFORMATION SECURITY MANAGEMENT POLICY

Introduction

This Policy applies to all L Lynch Plant Hire & Haulage Limited staff, including temporary staff, and contractors. The term "user" in this policy refers to all members of staff, including temporary staff, and contractors processing L Lynch Plant Hire & Haulage Limited information.

Definition

This policy is about how L Lynch Plant Hire & Haulage Ltd manages incidents that present a risk to information security within the company. This includes IT, business or operational related incidents.

It sets out clear responsibilities in respect of the relevant roles, escalation paths and criteria for handling any incident.

It is designed to protect L Lynch Plant Hire & Haulage Ltd information assets from compromise and prevent damage to IT assets and the L Lynch communication infrastructure. Its purpose is to underpin the company's ability to manage incidents successfully.

Objectives

The objectives of this policy are to:

- Protect the information assets of L Lynch Plant Hire & Haulage Ltd;
- Ensure adequate and appropriate response to incidents;
- Minimise the damage from incidents;
- Demonstrate that L Lynch Plant Hire & Haulage Ltd is maintaining effective control of incidents;
- Protect L Lynch Plant Hire & Haulage Ltd from damage to its reputation as a result of inappropriate management of information security incident;
- Provide a formal framework to ensure that L Lynch Plant Hire & Haulage Ltd learns important lessons from such incidents and can therefore feed these back into an improvement programme;
- Promote awareness amongst all users of their responsibilities in relation to protecting L Lynch Plant Hire & Haulage Ltd information and in reporting and managing incidents;
- Standardise communication between the users, contractors and the Senior Management Team with regard to the reporting and investigation of all incidents.

Definitions

An 'incident' is defined as any event or action that results in an actual and / or potential compromise of L Lynch Plant Hire & Haulage Ltd information or information assets and / or communications infrastructure.

A 'weakness' is a situation where there is potential for an incident to occur but where no incident has yet occurred.

Incidents and weaknesses can be categorised into business and operational related incidents and IT

related incidents. Appendix 1 contains examples of what these categories include.

Responsibilities

1. Every member of staff **MUST**:

- Read the L Lynch Plant Hire & Haulage Ltd Information Security Management Policy, and seek clarification from line management on any areas that are not clear;
- Report to the Directors any unusual or suspicious activities (or inactivity), weaknesses or events they identify, such as suspected or actual compromise of L Lynch Plant Hire & Haulage Ltd information assets or the corporate IT network;
- Comply with any instruction given, to prevent or manage an incident, by the L Lynch Plant Hire & Haulage Ltd Manager(s) and give any assistance required in the investigation of an incident.

MUST NOT:

- Attempt to resolve an Incident or Weakness themselves, but must report it to the Directors. The exception to this is that a user can take immediate action to secure an information asset that is at risk, for example by closing a door that shouldn't be open or locking an unlocked computer.
- Anyone who fails to act according to these responsibilities may be subject to disciplinary procedures as described in the Staff Handbook.

2. Third Parties / Contractors

- If L Lynch Plant Hire & Haulage Ltd engages contractors to deliver services and operations on its behalf, the terms and conditions set out in the contract will describe how incidents affecting the security of L Lynch Plant Hire & Haulage Ltd information must be reported;

Every Third Party / Contractor **MUST:**

- Ensure that all appropriate staff understand, are trained in and comply with the incident management procedures and responsibilities;
- Act upon incidents reported to them effectively and in a timely manner to maintain the confidentiality, integrity and availability of the L Lynch Plant Hire & Haulage Ltd information they handle;
- Report or escalate incidents as specified in their agreements/contracts to the relevant Manager(s);
- Co-operate fully with any investigation conducted by L Lynch Plant Hire & Haulage Ltd

INFORMATION SECURITY MANAGEMENT POLICY

This policy will be communicated to all employees and organisations working on our behalf and displayed at our offices and on our intranet. This policy is available to defined interested parties.

This policy will be reviewed annually or sooner by senior management to ensure its suitability. Where necessary it will be amended, reissued and communicated to all employees and people working on its behalf.

Liam Lynch, Managing Director

Date: 30/01/2020

INFORMATION SECURITY MANAGEMENT POLICY

Appendix 1

BUSINESS AND OPERATIONAL RELATED INCIDENTS

This will include (but not be limited to):

- Power outages;
- Theft and loss of IT hardware and software applications;
- Theft or loss of L Lynch Plant Hire & Haulage Ltd information held in physical format (including documents and files);
- Downloading, displaying or distributing racist, sexist or other material which seeks to denigrate any class of individuals;
- Downloading, displaying or distributing defamatory or other illegal material;
- An event likely to bring L Lynch Plant Hire & Haulage Ltd into disrepute;
- An event having a significant impact on the ability of L Lynch Plant Hire & Haulage Ltd to perform its duties;
- An event that is, or is likely to be of interest to local / national press;
- The potential for any of the above to occur (i.e. a weakness).

IT RELATED INCIDENTS

This will include (but will not be limited to):

- Malicious code attacks e.g. viruses, worms, etc.;
- Network attacks or Denial of Service (DOS) Attacks;
- Probes, scanning, etc.;
- Hacking type attacks or external intrusion;
- Telephone system failures;
- Inappropriate use of IT Assets, including harassment or illegal material;
- Unauthorised access to, or disclosure of, L Lynch Plant Hire & Haulage Ltd information;
- Compromise of integrity an information asset;
- Any alerts and suspicious activity on security critical systems, internal systems or applications and application platforms;
- The potential for any of the above to occur (i.e. a weakness).

GovCertUK Categories

The following list of specific incident types is provided by GovCertUK specifically for reporting purposes http://www.cpni.gov.uk/MethodsofAttack/report.aspx).

Some of these clearly overlap with the more general incident types listed above:

- Type 1: Network Probes and Scans;
- Type 2: Blocked Hacking Attacks;
- Type 3: Blocked Malicious Software Infection;
- Type 4: Actual Malicious Software Infection;
- Type 5: Successful Hacking Attacks;
- Type 6: Malicious Denial of Service Attacks;
- Type 7: Data Interception and Monitoring;
- Type 8: Other.