Information Security Incident Reporting Policy

Introduction

It is the policy of the Interr Security to handle information security incidents so as to minimize their impact on the confidentiality, integrity, and availability of the Company's systems, applications, and data. An effective approach to managing such incidents also limits the negative consequences to both the Company and individuals, and improves the Company's ability to promptly restore operations affected by such incidents.

It is especially important that serious information security incidents that may result in disruptions to important business processes are promptly communicated to the appropriate Senior Managers so that they are involved early in decision-making and communications. In addition, compliance with various law and regulations requires expeditious reporting of certain types of incidents.

While information security incidents are not always preventable, appropriate procedures for incident detection, reporting and handling, combined with education and awareness of the staff, can minimize their frequency, severity, and potentially negative individual, operational, legal, reputational, and financial consequences

Purpose

The goals of establishing a successful incident management capability include:

- Mitigating the impact of information security incidents.
- Identifying the sources and underlying causes of information security incidents and unauthorised disclosures to aid in reducing their future likelihood of occurrence
- Protecting, preserving, and making usable all information regarding the incident or disclosure as necessary for analysis and notification.
- Ensuring that all parties are aware of their responsibilities regarding information security incident handling.
- Protecting the reputation of the company.

Definitions

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorised access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy.

Examples of information security incidents:

- Computer system intrusion;
- Unauthorised or inappropriate disclosure of sensitive company data;
- Suspected or actual breaches, compromises, or other unauthorised access to Company systems, data, applications, or accounts;
- Unauthorised changes to computers or software;
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for Company work) used to store private or potentially sensitive information;
- Denial of service attack or an attack that prevents or impairs the authorised use of networks, systems, or applications;
- Interference with the intended use or inappropriate or improper usage of information technology resources.

While the above definition includes numerous types of incidents, the requirement for central security incident reporting, regardless of malicious or accidental origin, is limited to serious incidents as defined below. Occurrences such as incidental access by employees or other trusted persons where no harm is likely to result will usually not be considered information security incidents.

A serious incident is an incident that may pose a substantial threat to Company resources, stakeholders, and/or services.

An incident is designated as serious if it meets one or more of the following criteria:

- Involves potential, accidental, or other unauthorised access or disclosure of sensitive institutional information (as defined below);
- Involves legal issues including criminal activity, or may result in litigation or regulatory investigation;
- May cause severe disruption to mission critical services;
- Involves active threats;
- Is potentially widespread;
- Is likely to be of public interest;
- Is likely to cause reputational harm to the company.

Scope

This policy is platform and technology neutral, and applies to the entire Company. Specifically, the scope of this policy encompasses:

- Company staff;
- Third-party suppliers or trading partners who collect, process, share or maintain Company data, whether managed or hosted internally or externally;
- Personally owned devices of members of the staff that access or maintain sensitive data;
- All users of Company IT resources must report all information security incidents to their Head of Department or line manager, who will do so on their behalf.;
- Any event that appears to satisfy the definition of a serious information security incident must be reported to the Data Commissioner;
- It is expected that incident reporting, from identification to reporting to control (if necessary), will occur within 24 hours;
- Some information security incidents may also be criminal in nature (e.g., threats to personal safety or physical property) and should immediately be reported to the ISO/CEO/DHRC concurrent with the incident notification;
- To avoid inadvertent violations of British law, individuals and departments may not release information, electronic devices, or electronic media to any outside entity, including law enforcement organisations, before making the notifications required by this policy.

Reporting

All staff must report serious information security incidents to their line manager and HR immediately after becoming aware of the incident.

Line manager and HR will initially evaluate and respond to non-serious incidents, and coordinate a response to risk assessments and audit requests. Investigations will be co-ordinated by the HR & Compliance Director, Information Security Officer and IT & Systems Administrators using the lessons learnt to also develop and implement policies, procedures, communications, and educational awareness programs consistent with Company-wide guidance.

The HR and Compliance Director (Data Protection Officer) must report suspected serious incidents (reported to or identified by them) within the 24-hour timeframe to the ISO and CEO. Additionally, the Data Protection Officer will coordinate and submit details of a serious incident/data breach to the ICO and other required authorities as well as any individual potentially impacted.

When an incident involves the types of sensitive information below, they must also report the incident to the following parties:

- Third Party suppliers and Contractors: the company has an interest in all data, regardless of how or where it is stored, transmitted, or processed. The reporting requirements of this policy apply to third parties that are contractually bound to limit the access, use, or disclosure of Company information assets. These third party suppliers or entities shall report potential or actual incidents to the Company as per their instructions.

Any member of staff or contractor working behalf of the Company has a duty to report the loss, suspected loss or unauthorised disclosure of any Company information asset to the HR and their line manager.

Any employee found not to have reported a security incident may be subjected to disciplinary action in line with Interr's disciplinary procedures.

Policy Review and Assessment

This policy may be amended by Interr at any time in order to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
July 2022