Information Security Incident and Events Reporting Policy

Introduction

It is the policy of the Interr Security to handle information security incidents and events 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 and events 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 and events are not always preventable, appropriate procedures for incident detection, reporting and handling, combined with staff education and awareness, can minimize their frequency, severity, and potentially negative individual, operational, legal, reputational, and financial consequences.

All personnel and users have also a responsibility not just to report any information security incidents but also information security events as quickly as possible to IT@interr.com as soon as possible to prevent or minimise the effects of information security incidents.

Purpose

The goals of establishing a successful incident management capability include:

- Mitigating the impact of information security incidents and events.
- 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 all relevant evidence is gathered, recorded, preserved and maintained in a form that will withstand internal and external scrutiny and external bodies or data subjects are informed as required.
- Protecting the reputation of the company.
- Ensuring that all parties are aware of their responsibilities regarding information security incident handling.

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 events (not limited to):

- Access violations;
- Suspected malware infections;
- Human errors;
- Non-compliance with the information security policies;
- Breach of information confidentiality, integrity or availability expectations;

- Systems change that have not gone through the change management process;
- Vulnerabilities;
- Breaches of physical security measures.

Examples of information security incidents (not limited to):

- 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;
- Misuse or loss of any hard copies or documents printed or written on paper; speech, voice recording, photographs or any other physical documents.

While the above definition includes numerous types of incidents and events, 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.

Incident Reporting

All staff must report serious information security incidents to the Operations Control Centre immediately after becoming aware of the incident. The operations control centre will escalate it to the relevant management in the organisation

Management 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 or governing bodies as well as any individual potentially impacted.
Where required, the company may involve legal advice or law enforcement early in any contemplated legal actions and take advice on the evidence required.

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 security information incident that may be part of a potential disciplinary, criminal activity or for legal purposes must be approached with care and must be stored in a secured controlled environment and treated as information level security – 3. Digital evidence can be exceptionally fragile and must be handled carefully to remain admissible. Preservation of evidence is required to preserve the integrity of the evidence (tampering) and an audit trail of all processed data applied to collect evidence is required. This included demonstrating how and where from the evidence has been obtained, under whose responsibility and where and how it will be stored. Evidence collected must include passwords and encryption keys needed to access password protected or encrypted areas of storage containing electronic evidence.

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.

Event Reporting

All staff must report any information security events to IT@interr.com immediately after becoming aware of the event.

Management will initially evaluate and respond and coordinate a response to risk assessments and audit requests. If any investigations are required, they 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.

Protection of logs, event and security information

Access to Interr's network, systems and communications shall be logged and monitored to identify potential misuse of systems or information, alterations, edited, deleted, overridden, etc. Logging activities shall include regular monitoring of system access to prevent attempts at unauthorized access and confirm access control systems are effective. Log servers and documents shall be kept secure and only made available to relevant personnel. These logs shall be kept as long as necessary or required for functional use, to satisfy audits and /or appropriate regulatory requirements or law. Some audit logs may be required to be archived as part of any requirements to collect and retain as evidence for a maximum of 3 years.

Interr's information systems (servers, workstations, firewalls, routers, switches, communications equipment, etc.) shall be monitored and logged to:

- Ensure use is authorized
- Manage, administer, and troubleshoot systems
- Protect against unauthorized access
- Verify security procedures and access
- Verify system and operational security
- Comply with Interr's policies and procedures
- Detect and prevent criminal or illegal activities

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit logging information to:

- Determine the activity that was performed
- Who or what performed the activity, including where or on what system the activity was performed (subject)
- Systems and objects involved
- When the activity was performed
- Alterations or deletion or edition or over riding of past events
- Status (such as success vs. failure), outcome, and/or result of the activity

The frequency of review logs shall be determined according to the sensitivity of the information stored, the function of the system, and other system requirements as determined by the Company. This is to:

- Ensure events are properly classified
- Review logging for performance delays
- Ensure compliance related logging cannot be bypassed
- Verify access to log files is properly restricted
- Assist with investigations and compliance with relevant authorities

Logs shall be protected against any security risks by permitting only the authorised personnel to have access to these logs and by completion of internal audits by independent personnel.

- Protect the information held within system audit logs in accordance with its Information Classification as stated on Interr's Information Handling policy.
- Review the activity logs of privileged users and system administrators on a quarterly basis by the Information system security managers and administrators and reviewed by the compliance team, to ensure that privileged users remain impartial and maintain accountability for the users.
- Only access, monitor, or analyse logs, network connections, or location information of individuals for legitimate business and job-related purposes.
- Keep such information confidential, and not disclose such information to others unless there is a job-related or legal requirement to do so.
- All security logs shall be backed-up and archived as required.
- Administrators shall take appropriate precautions to prevent security logging from being deactivated, modified or deleted.
- Logs, logging facilities and log configuration tools must be protected so that only authorised administrators have access and no end users may delete or alter logs. If separate log archiving facilities are used, the administrators for these facilities should be different from the administrators for the systems generating the logs in order to prevent misuse by system administrators. Access to logs must be granted on a strict need-to-know basis.
- System clocks are used to record the date and time of events in log entries, and the correct setting of clocks is important to ensure their accuracy. Inaccurate audit logs may hinder investigations and damage the credibility of log entries used as evidence.
- The confidentiality and integrity of the archived logs also need to be protected. Use only those computing resources that they have been authorised to use, and use them only in the manner and to the extent authorised.
- Do not interfere with the intended use or proper functioning of information technology resources, or gain or seek to gain unauthorised access to any resources.
- Do not circumvent or bypass security measures, requirements, or any standard protocols in place to ensure the confidentiality, integrity, and availability of Interr systems and networks.
- Asset log will only be controlled and monitored by the authorised personnel and reviewed quarterly by the compliance team to ensure accountability of all assets.

Requirement

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.

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
January 2024