Information Handling Policy

Introduction

This Information Handling Policy is a sub-policy of the Information Security Policy and sets out the requirements relating to the handling of the Company's information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation, which would otherwise occur.

Security classification

Each information asset category will be assigned a security classification by the asset owner, which reflects the sensitivity of the asset and information security needs of the organisation based on confidentiality, integrity and availability and relevant interested parties requirements, according to the following classification scheme:

- **Level 1 – General** (unmarked Documents) – Non-sensitive documents such as public bulletins and information are available for open use – no form of marking is required on such documents.
- **Level 2 – Restricted** – (internal use only) - While not an official marking, this may be used to identify Information such as policy, guidance or procedures, non-sensitive documentation that are not normally disclosed publicly.
- **Level 3 – Secret** (official – sensitive) - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to Interr or a commercial partner if improperly accessed.

Any information which is disclosable under the Freedom of Information Act 2000 will be classified as public. Any data which is classified as sensitive personal data under the Data Protection Act 2018 (or its successor legislation) will be classified as Secret.

Access to information

Members of the Company will be granted access to the information they need in order to fulfil their roles within the Company. Staff who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

Access Roles / Identities

Users must only use business systems for legitimate use as required by their job and in accordance with the procedures for those systems. A nominative and individual privileged user account must be created for administrator accounts instead of generic administrator account names. Privileged user accounts can only be requested by the senior management team and must be approved prior by the CEO.

Systems will be capable of logging events that have a relevance to potential breaches of security. User access will be subject to management or IT team checks.

User identities are defined by Interr as:

Standard User

Minimum level access to systems and platforms they need to perform their job and has zero administrative privileges in any capacity and have access to level one information.

Elevated Standard User

Elevated level access to systems and platforms they need to perform their job and may have limited administrative privileges, such as setting up new starers on the system and have access to level two information.

Privileged User – Super Admin

A privileged user is a user who has an elevated level of access to a network, computer system or application and is authorised to perform functions that standard or elevated standard users are not authorised to perform.

Non Human Entities

Identities assigned to non-human entities often refer to unique labels or identifiers assigned to machines, devices, or artificial intelligence systems for the purpose of recognition, tracking, and communication within a networked environment. These are managed by having the most up to date system updates, security patches, encryption or authenticator protocols where required (i.e, internet banking), firewall and antivirus detection systems.

Roles and Responsibilities

Executive Management:

These executive level roles generally are responsible for overseeing the enterprise information security strategy that ensures information assets are protected.

The oversight responsibilities include the following (not limited to):

- Overseeing the process of handling required policy exceptions and recommended appropriate actions
- Ensuring appropriate risk mitigation and control processes
- Overseeing the development, enforcement and implementation of the company information systems

Interr's Executive Management responsible for the above are:
Mick Tabori (CEO)
Chris Dean (CFO)

Information Security Officer / Data Protection Officer

The Information Security Officer/ Data Protection Officer Role is responsible for coordinating all activities related to information security management in the Organization.

The oversight responsibilities include the following (not limited to):

- Definition and supervision of the Information Security Management System
- Contacting authorities and groups of interest in the area of ISMS
- Coordinating the risk management process
- Managing data protection within the company

Interr's Information Security Officer responsible for the above is:
Chris Dean (CFO)

Interr's Data Protection Officer responsible for the above is:
Elena Klopanova (DHRC)

Information System Security Managers and Administrators:
Responsible for the design, implementation, management, and support the review of the organization's security policies, standards, baselines, procedures, and guidelines, together with the CEO, ISO, DPO and external SMEs.

The oversight responsibilities include the following (not limited to):

- Development and implementation of information security training
- Documentation and implementation of security policies, guidelines and systems
- Coordinating and responding to any information security breaches in the confidentiality, integrity or availability of information assets
- Identifying, evaluating and reporting on information security risks

Interr's Information System Security Management responsible for the above are:
IT & Systems Administrator – Ben Pinner (Client Director)
IT & Systems Administrator – Mateusz Kiezel (Systems and Projects Manager)

Data Owners:
Owners is a group of employees or an individual who are officially designated as accountable for any specific data that is transmitted, stored, or used on any company systems. They can be the owners, information owner or system owners who have budgetary authority.

The oversight responsibilities include the following (not limited to):

- Ensuring that appropriate security—consistent with the organization's security policy—is implemented in their information systems
- Determining appropriate sensitivity or classification levels
- Determining access privileges
- Having an understanding of legal and contractual obligations surrounding information assets

Interr's Information System Data Owners responsible for the above are:
Finance Manager (**Finance Team**) – Candice Hamilton
HR Manager (**HR Team**) – Lucia Hermida
OCC Director (**OCC Team**) – Barry Desborough
UK Retail Operations Director (**Retail Ops Team**) – Yolande Frederick
Client Director (**Corporate Ops Team**) – Jonathan Dennison

Data Custodians:
A function that has "custody" of the system/databases, not necessarily belonging to them, for any period of time. Usually network administration or operations (those who normally operate the systems for the owners).

The oversight responsibilities include the following (not limited to):

- Implementing all appropriate technical or physical safeguards to protect the confidentiality, integrity and availability of information assets
- Understanding how information assets are stored, processed and transmitted

Interr's Information Data Custodians responsible for the above are:
Elena Klopanova (DHRC)
IT & Systems Administrator – Ben Pinner (Client Director)
IT & Systems Administrator – Mateusz Kiezel (Systems and Projects Manager)

Users:
Responsible for using resources and preserving availability, integrity, and confidentiality of assets; responsible for adhering to security policy.

Interr's Users responsible for the above are:
All Interr Employees
Anyone who comes into contact with Interr data

IS Auditors:
Responsible for providing independent assurance to management on the appropriateness of the security objectives and determining whether the security policy, standards, baselines, procedures, and guidelines are appropriate and effective to comply with the organization's security objectives.

Interr's Users responsible for the above are:
Elena Klopanova (DHRC)
IT & Systems Administrator – Ben Pinner (Client Director)
IT & Systems Administrator – Mateusz Kiezel (Systems and Projects Manager)
External IT Partners - IP Integration
Information Security Penetration and Compliance Testing Partners - KryptoKloud
SIA ACS and ISO Certification Auditing Partners - British Assessment Bureau Auditors

Disposal of information
Great care needs to be taken to ensure that information assets in all forms, physical and logical are disposed of securely. Confidential paper waste must be disposed of in accordance with formal Company procedures.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Company, unless the disposal is undertaken under contract by an approved contractor, as detailed in the policy on the Secure Disposal of IT Equipment.

Removal of information
Company data, which is subject to the Data Protection Act or which has a classification of Level 2 - Restricted or Level 3 – Secret, should be stored using Company facilities or with third parties subject to a formal, written legal contract with the Company, wherever possible. In cases where it is necessary to otherwise remove data from the Company, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Level 3 – Secret data in electronic form must be strongly encrypted prior to removal. Secret data must never be removed except with the explicit written permission of the data owner. (See the Cryptography policy). Particular care needs to be taken when information assets are in transit.

Using personally owned devices
Data subject to the Data Protection Act must never be stored on personally owned devices. Data classified as sensitive under the Data Protection Act must neither be stored on nor processed using personally owned devices.
Personally owned devices should not be used for the storage or processing of any other information classified as strictly confidential or above without the explicit written permission of the data owner. Appropriate security measures must be taken when using personally owned devices to process or store any Company data.

Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended. Staff offices should be locked when empty.

Backups

Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

Exchanges and transfer of information

Whenever personal data or other confidential information is transmitted to or exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

Information classified as Level 2 - Restricted may only be exchanged electronically both within the Company and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified, as Level 3 - Secret may not be transmitted electronically except with the explicit written permission of the information owner.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission. Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Staff or contractors of the Company must not disclose nor copy any information classified as Level 2 - Restricted or above unless they are authorised to do so.

Electronic transfer

The company uses HTTPS websites for web transactions, ensure the integrity and confidentiality of data exchanged between users and servers. Additionally, firewalls, antivirus software, and intrusion detection systems are implemented to detect and thwart potential cyber attacks. Regular software updates and patches are scheduled to address vulnerabilities that could be exploited by malicious attacks. User authentication methods, like two-factor authentication is in place to provide multiple forms of identification. No staff should be using any public network and are encourage do use hot spotting or only accessing data when using a safe network. An online training regarding GDPR and email correspondence is required to be completed by all Head Office staff on annual basis.

Physical transfer

The company does not permit the use of storage media (such as usb and memory disks, not limited to) and discourages printing of any documentation unless absolutely necessary.

Should any paper or any data of sensitive materials have to be transferred via an external provider, Interr shall ensure the provider has the appropriate security measures in place and verify the recipient of the information. Any such data will be sealed in a sealed and signed envelope/ box to prevent from any potential tampering and access.

Verbal transfer

All Interr employees must understand how their actions may affect the information security and are requested to use discretion during verbal exchanges at work, in public areas or within their home environment.

Data leakage prevention

Interr's documents containing sensitive information will be marked with an embedded security classification (level 3) to facilitate technical measures within boundary controls to prevent data leakage and/or loss and indicate to information users its classification and handling requirements.

The following boundary controls will implement technical measures to prevent data loss:

- Data at rest on portable computers will be protected from theft/loss by use of assured encryption.
- Boundary controls shall be cognisant of the levels of classification that are/are not appropriate for each egress path. For example, some classifications may be permitted for transmission over secure email systems, or for upload to secure websites within the Company's network.
- Boundary controls will block content that obfuscates electronic security classifications by encryption (e.g. zipped files).
- Blocking user actions or network transitions that expose sensitive information.
- Monitor the channels of data leakage/loss and acting to prevent information from leaking (i.e. quarantine emails containing sensitive information).
- No forwarding of company emails to personal email addresses is allowed. The forwarding rule is set up and monitored.
- Maximum of 100 persons within one email address rule set up.

Reporting losses

Any member of staff or contractor working behalf of the Company has a duty to report the loss, suspected loss, leakage or unauthorised disclosure of any Company information asset to the HR & Compliance Director.

Policy Review and Assessment

This policy may be amended by Interr at any time 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