IT & Information’s Technology Security Policy & Procedures

H&S | UK

The Company's Scope

The company seek to ensure that all technology and information assets provided and managed by us are adequately protected against security threats including any compromise, loss, unauthorised access / disclosure or any other type of misuse.

This policy provides written guidance to all the company's employees' who use or have access to the IT facilities. It is designed to help them to ensure they are aware of, and fully comply with, the requirements placed upon them by this policy and are aware how to work in a professional, security aware manner.

This policy applies to all employees of the company, plus any freelance workers, sub-contractors or other third party persons who may have authorised access to the company's IT infrastructure.

This policy should also be read in conjunction to the company's Data Protection Policy.

1.0 Introduction

This document sets out the Information Technology (IT) Policy for the company, for the protection of its IT systems and defining baseline responsibilities for IT security, equipment and file storage. "IT systems" refers to any of the networks, hardware including portable media, system and application software, communication components including telephone and WAN systems, documentation, physical environment and other information assets. It does also include IT systems not connected to the company's networks but only where information is stored for business means.

1.2 This Policy covers all staff across all sites and any separate networks or equipment's provided for company by third parties and other third party Information Management and Technology in order to manage the company's websites and storage systems.

1.3 The equipment covered by this policy includes:

- **Network Infrastructure** – The equipment housed internally to provide the IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems and devices and remote access systems.
- **Desktops** – Personal Computers (PCs) issued or provided to staff in the course of carrying out their duties
- **Laptops/Netbooks** - Portable Personal Computers issued or provided to staff in the course of carrying out their duties
- **Mobile Phones/Smartphones** - Digital communication devices issued or provided to staff in the course of carrying out their duties
- **Desk/Conference Phones** – Telephones/Voice Communication devices connected to the Network Infrastructure including desk telephones, conference telephones, analogue telephony adaptors, DECT telephones (cordless)
- **Media/Portable Media** – Electronic Storage Devices such as DVDs, CDs, memory sticks and hard drives issued or provided to staff in the course of carrying out their duties
- **External Communications Infrastructure** – Equipment used to connect the company to the external world including the Wide Area Network, analogue telephone lines, digital telephone lines, leased lines, Ethernet first mile circuits, ADSL circuits, SDSL circuits and all related equipment and services.
- **All related Facilities& Estates** controlled IT media used in meeting rooms.

1.4 The objective of this policy is to ensure: -

- The confidentiality of data and information assets are protected against unauthorised disclosure and incidents are promptly reported
- The integrity of data and information assets so that they are protected from unauthorised or accidental modification
- The availability and accessibility of IT systems as and when required by staff

1.5 This policy sets out the principles of IT security including the maintenance, storage and disposal of data and explains how they will be implemented by the group to ensure there is a centralised and consistent approach to IT security.

1.6 One of the aims of the policy is to raise awareness of the importance of IT security in the day to day business.
The policy supports the business objectives of ensuring that the security, integrity and availability of IT systems are balanced against the need for staff to access systems and services that are necessary for their job, within the limits imposed by this policy.

It will also help to protect data from misuse and to minimise the impact of service disruption by setting standards and procedures to manage and enforce appropriate IT security.

1.7 The policy supports the legal obligations of the company to maintain the security and confidentially of its information, notably under the Data Protection Act 1998, the Copyright Patents and Designs Act 1988 and the Computer Misuse Act 1990, and also supports adherence to information governance standards set by the Department of Health (DH) and GDPR Regulations.

2.0 Responsibilities

Defining responsibilities ensures that all users of IT systems are aware of their responsibilities to minimise the risks to IT security and operations.

2.1 The Senior Management Team is responsible for ensuring that:

- Electronic filing systems and documentation are well maintained for all critical job functions to ensure continuity;
- No unauthorised staff are allowed to access any IT systems in any location, as such access could compromise data integrity;
- Named individuals are given authority to administrate specific computer systems according to their job function and role following the principle of least privilege;
- Robust disaster recovery and business continuity procedures are in place with our IT provider
- All current and new users are instructed in their security responsibilities;
- Procedures are implemented to minimise the groups exposure to fraud, theft or disruption of its systems; these include segregation of duties, dual control and staff rotation in critical susceptible areas.

2.2 The IT companies employed by the company have the following responsibilities:

- Day to day responsibility for the management and security of the systems, equipment and services, with specific technical responsibilities being allocated across the company and to outsourced service providers.
- To make sure all users they deal with are aware of this policy and to ensure that users are reported to Senior Managers if they feel the policy is not been abided by.
- Monitoring and reporting on the state of IT security within the group
- Developing and enforcing detailed procedures to maintain security access to all systems.
- Ensuring compliance with relevant legislation, policies and good practice for all internal systems.

- Monitoring for actual or potential IT security breaches for all internal systems. And reporting to the appropriate people as need be.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence.

2.3 The HR department or IT director is responsible for ensuring that:

- All staff sign confidentiality (non-disclosure) agreements, undertakings as part of their contract of employment, and any contactors, temporary staff (including agency staff) and appetencies sign company's confidentiality undertaking before they are permitted to use IT systems.

3.0 Security

3.1 Technical security measures will be put in place to protect all systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.

3.2 Email and internet use will be governed in accordance with the Email and Internet policy.

3.3 Allocation of accounts to temporary workers using a generic username that cannot be mapped back to the user will not be allowed.

3.4 All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the company directors.

3.5 All IT equipment, including virtual systems, will be uniquely identified and recorded.

3.6 Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking and eating is not permitted in these areas.

3.7 Records of all faults and suspected faults will be maintained.

3.8 Access to premise server/communications rooms will only be with the express permission of a senior manager.

3.9 Passwords will be changed every 90-day period. They will need to be of suitable strength to provide adequate protection for the systems that are accessed.

3.10 Any suspected breach of passwords must be reported to the employees' line manager as soon as the employee becomes aware.

4.0 Software Protection

4.1 Only licensed copies of commercial software or in house developed software are used by group. Users must not install ANY externally developed software on any equipment without prior approval of director.

4.2 All users are reminded it is a criminal offence to make or use unauthorised copies of commercial software and that offenders may be liable to disciplinary action.

4.3 Software products required by any department should be approved by an internal review prior to purchase. Unless otherwise directed all software purchasing and licensing will be carried out via our IT providers, and users must follow any instructions issued with regard to specific software or applications.

4.4 The company will minimise the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software and ensuring firewall policies follow appropriate guidelines. Users must report any detected or suspected viruses, Trojan, spyware or malware on their computers immediately.

5.0 Disposal/Reallocation of Equipment

5.1 Equipment issued to an individual user must not under any circumstances be reallocated within a department (or any other user) and must always be returned to the person in charge of IT for reallocation to ensure correct management of sensitive data

5.2 Where equipment is obsolete to the business but is still in working order and is deemed to be of use to private individuals, that equipment may be offered charities without any guarantees or warranties.

5.3 Where the equipment is deemed to be of no use, it will be either disposed of by a registered, certified company, ensuring that any hard drives have been wiped or removed. The PC / Laptop / Tablet will be disposed of in accordance with the Waste Electrical and Electronic Equipment Directive (“WEEE”).

R. Chappell
18/04/2022
Next Review: 18/04/2023