IT Cyber Security Policy

Revision History:

No	Author/Reviewer/Owner	Date	Status (Draft/Published)	Comment
IT-P01	Asim Syed	Jun 22	Jun 22	Document review and transfer to SharePoint

POLICY CONTENTS PAGE

1. Purpose

This policy outlines Peoplesafe's Information Technology Cyber Security policies, procedures, and the responsibilities of employees using IT systems and infrastructure.

This policy is mandatory. Any breach of the policy may result in disciplinary action being taken under the Disciplinary Procedure.

Any breaches of security and non-compliance must be reported to the IT department itsupport@peoplesafe.co.uk or by calling on 020 8786 3366. Serious breaches should also be reported directly to the IT Director, asim.syed@peoplesafe.co.uk and the Compliance Director / Data Protection Officer, ricardo.pombo@peoplesafe.co.uk

Goals:

- Confidentiality of information is maintained.
- Information is protected against unauthorised access.
- Information is not disclosed to unauthorised persons through deliberate or negligent action.
- The integrity of information is maintained by protection from unauthorised modification.
- Information is available to authorised users when needed.
- Regulatory and legislative requirements are met.
- Contingency plans are produced and tested to ensure business continuity is maintained.
- All breaches of information security and suspected weaknesses are reported, investigated and appropriate action taken.

2. Scope

To ensure that all IT systems operated by Peoplesafe are secure and comply with the requirements of International Standard for Information Security ISO27001 and Cyber Essentials Plus.

This policy is applicable to all employees and third parties with access to company equipment and are responsible for ensuring the safety and security of the company data and equipment:

- Employees must ensure that no unauthorised person has access to any data held by the company.
- Employees must not deliberately or negligently corrupt, damage or destroy company data, software and hardware. This includes the spread of viruses or similar computer programs.
- Employees will be given access passwords to the required IT systems. These passwords must not be disclosed to anyone, including other members of staff. They must not be written down and they should be changed regularly.
- Employees must not install or download software packages and games on to company PCs.
- Any employee found to be storing personal files may be asked to remove them. Large files such as photographs or videos must not be stored on company property or on the company network.
- Any files received on any media or files received by electronic mail must be virus checked before being loaded on to a company PC.
- All employees must read, understand and sign to acknowledge that they have read and accepted this policy and the specific requirements.

3.0 Information Security Roles and Responsibilities

Head of Departments:

- Ensure staff are aware of the Information Security Policies.
- Consider IT Cyber Security Policy when employing new staff, contractors and third parties.
- Ensure staff are trained in cyber security and use of information resources.
- Report promptly any suspected breaches of the IT Cyber Security policy to the IT department.

Staff & Contractors:

- Comply with IT Policies.
- Prevent unauthorized disclosure of the data.
- Protect the confidentiality of their login credentials, user ID & passwords.
- Report promptly any suspected breaches of IT Cyber Security policy to the IT department.

IT Department:

- Formulate IT Policies.
- Oversee the implementation of cyber security throughout the company.
- Review and approve the cyber security elements of business cases for new systems and products.
- Assess risks and make decisions involving information system risk management.
- Ensure that operating procedures are kept up to date.
- Ensure that cyber security training & awareness updates are communicated to the users.
- Business Continuity Procedure is kept up to date.

The IT Director, along with the DPO has specific responsibilities to maintain the structure of the IT Cyber Security policy, investigate breaches of the Policies.

3. Conditions of Use

Employees will sign to agree compliance with all company policies and will have access to full copies of them when they accept their contract of employment with the company.

Employees of the company who fail to follow all aspects of the *IT-P01 IT Cyber Security Policy* may be subject to the company's disciplinary procedures.

Infringement of civil or criminal legislation shall be reported to the appropriate external entities. In addition to disciplinary action, the instigator/owner of the unauthorised copyright material or inappropriate digital information may face legal penalties.

3.1 Company Regulations Compliance

Existing company rules and policies apply equally to the use of all electronic services. This IT Cyber Security Policy underpins other IT policies and procedures

4. Network Infrastructure Controls

4.1 Network Security

- Company owned Laptops, PC's and Tablets are only allowed to connect to the corporate network.
- If remote access is required from outside the office, specific permission must be sought from the company's IT department.
- All employees and third-party contractors are required to access the public internet via the firewall.
- All employees must never move or connect network cables in the office. Network cables are only to be moved or connected by a member of the IT team, or with the explicit consent and instruction given by the IT team.
- All employees must not connect any unauthorised devices to the network cables in any office.
- Company maintains segregation in the networks for general office, core server room and voice data.
- All power and network cables from external sources are secured underground and sealed to protect against any interference, interception and damage.

4.2 Network Monitoring and Reporting

- Network traffic is monitored in order to counter unusual traffic patterns and internal or external sabotage attempts.
- The introduction of unauthorised user equipment, tampering with company equipment, unauthorised changes to network settings, introduction of unauthorised software and provision of electronic, wiring, or wireless devices that will introduce, change, bridge or route network access paths is a serious breach of this Policy.

4.3 Securing Application Services

- The company's firewalls maintain security policies in place to restrict incoming and outgoing traffic. This is coupled with sophisticated threat protection and intrusion detection & prevention systems. The core server infrastructure is based in Epsom's data centre.

- Information involved in application service transactions are protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay. The below are in use to protect application transaction information:

    - Secure electronic signature.
    - Encryption by security protocols (i.e., TLS).
    - Real time monitoring by database monitoring tool.

4.3.1 Protection Against DDoS (Distributed Denial of Service)

To mitigate against DDoS attacks, the company maintains filters in place with the ISP (internet service provider) to block such attacks and are continuously monitoring for change in DDoS attack patterns.

4.3.2 Protection Against Ransomware & Cyber Threats

- Security controls are in place to filter all incoming & outgoing emails and block any suspicious or malicious attachments.
- Restrictions are in place to block users from running any executable files from the location where the ransomware virus may install and spread on the network.
- IT Systems are locked down and run the latest up to date security endpoints which specifically protects against ransomware attacks and malicious applications. These endpoints are updated every 30 minutes for the latest signatures.

4.4 Reporting Information Security Events

- The IT systems and infrastructure are proactively monitored 24/7, for any abnormal traffic patterns using a set of advanced dashboards, alerts & reporting.
- All the users' internet traffic is monitored and filtered.
- Users are only allowed to go on business related websites and are restricted from downloading any unauthorised software.
- IT SOC use a variety of sophisticated security systems to proactively scan networks & systems for threats:

1. Malware
2. Viruses
3. Abnormal traffic patterns
4. DDoS attacks

- All traffic is monitored at the perimeter level using secure firewalls which consists of strict security policies and access controls. Filters & protection in place to mitigate against cyber-attacks.
- Security endpoints reside on all the servers and workstations which monitors all malicious activities on the machines to automatically protect and notify against any vulnerabilities and Cyber-attacks

5. Physical Controls

5.1 Physical Security

- Access to data held on the company IT systems is minimised by restricting physical access to Peoplesafe building.
- Access to the perimeter is restricted by a multi-tier security system of the company's building Security and CCTV.
- Where information is kept in Peoplesafe office, access to buildings is restricted by ensuring that security doors are closed properly, and door access cards are used.
- Physical sets of keys are only provided to designated Peoplesafe employees, who have been provided with a copy of this document signed the Acknowledgment of Acceptance.
- Doors and windows must be secured at lunch times, overnight and at all times when the office is left unattended.
- Visitors must be accompanied at all times and signed in and out of the premises on arrival and departure.
- Access points such as delivery and loading areas are controlled to avoid unauthorized access by CCTV cameras and video doorbell.
- Any IT asset must not leave the building without prior written authorisation by the IT Director.
- Company maintains fire warden; all the fire safety equipment is in place which are regularly serviced.
- Company work premises are quite higher than the ground which provides initial protection from flood.
- Proper ventilation of the building is maintained and serviced regularly which maintains air circulation.
- Disaster recovery site is maintained to escape other environmental threats.

5.2 Alarm Receiving Centre

The ARC (Alarm Receiving Centre) meets BS8484 and BS5979 requirements and operates 24/7 in a secure environment with strict access controls.

- ARC team and designated personnel are authorised to enter the ARC.
- Anyone entering the ARC are required to press the buzzer at the ARC entrance.
- ARC controllers carry out a visual check via the intercom before granting admission to ensure that the person is on the authorised list and not under duress.

5.3 Protection of Sensitive Areas

Access to network cabinets and datacentre areas are restricted to named IT personnel and supervised contractors. Access rights or keys will not be released to other individuals. Key IT locations and resilient back-up areas are maintained and secured with additional environmental and fire alarm equipment as described in detail in the Business Continuity Plan.

The data centre is not built near water pipes. Smoke alarms are placed in every floor adequately, fire detection test is completed weekly.

6. Computer Controls

6.1 Computer Security

- Only company desktops and laptops are permitted to connect to the corporate network.
- Only company PCs have access to the corporate domain and resources.
- All the PCs and users' activities are monitored and recorded to deter inappropriate use.
- All the PCs are locked down to restrict employees from installing any software.
- The use of utility programmes is controlled and monitored by the IT team. Download, installation, and use of those privileged utility programmes are restricted to the IT team.
- All the PCs are monitored for unauthorised applications and utility programmes.
- Regular Windows security updates and patches are centrally deployed to PCs.

6.2 Data Storage

- All employees must abide by the rules of the Data Protection Act, the General Data Protection Regulations and the Computer Misuse Act. Failure to do so may cause the Company to incur a fine of £17.5 million or 4% of the Company's global annual turnover of the previous financial year, whichever is higher.
- Access to individual file shares will only be granted following a written approval from the Head of department.
- Storage of data on PC or Laptop's C: drive is discouraged, and all users are not permitted to store files on PC or Laptop's C:\drives as in the event of failure, all data stored on the C: drive is lost as it is not backed up.
- All information related to company business to be stored on the company's shared drives or on M365 OneDrive (including SharePoint). This is a secure storage area which is regularly backed up and is therefore resilient to failure.
- No personal files are to be stored on company's PC or Laptop and network drives.
- Set thresholds are in place to enforce responsible use of expensive file storage resources. IT department regularly monitors employees file store and traffic.

6.3 Screen Locking

- Computers must not be left unattended with screen unlocked when logged in at any time. This applies to all employees regardless of their working location e.g., Home, Office or elsewhere.
- Employees must ensure that they have logged off or locked the PC when they leave the PC unattended.
- Computers will automatically lock the screen after 5 minutes of inactivity.
- Employees must ensure they have shut down the PC and Monitor when they leave work.

6.4 Passwords

- Passwords given to the employee are for their use only.
- Users must not use browser password or credential savers.
- Passwords must not be written down or given to other employees or any other person under any circumstances.
- Passwords must be a minimum of 8 case sensitive characters and should be a combination of upper/lower/numeric and special characters such as **#@?!$&** etc. Passwords must include at least three different character types, or they will not be accepted.
- Change of IT Systems passwords is enforced every 90 days.
- Password history is enforced to avoid using the previous four passwords.
- Passwords are not to be shared under any circumstance. If the employee is off sick or away on leave, the Line manager or Team Leader must contact the IT Help Desk to request managerial access to the employee's computer.
- Employee accounts will be locked after 4 invalid login attempts. A ticket will need to be raised with the IT Helpdesk to unlock the account.
- Passwords for documents which have been password protected should only be shared with those employees who have the right to access the document. When sharing a password for a document by email, the password should be sent separately to the document it relates to.

6.5 Memory Sticks and Removable Media

- Company does not allow the use of any removable media.
- Company supplied encrypted memory sticks are to be used upon authorisation.
- Company data must not be transferred to non-company devices such as home PC / Laptop and unauthorised USB media.

6.6 Anti-Virus Software

- All internal PCs and servers maintain Bitdefender antivirus software. No user is permitted to tamper with or remove this software.
- Automatic online updates will detect and deal with a high percentage of known viruses and malicious software. From time-to-time new virus patterns may emerge in advance of antidote software and notification of these viruses and common hoax viruses will be circulated via email, from the IT department.
- All files received on DVD disc or USB stick or received via electronic mail will be automatically checked for viruses before being used on company equipment. You must not intentionally introduce/send or download files or attachments which contain viruses, or which are meant to compromise the company's IT systems.
- If a virus is suspected, the IT Help Desk must be informed immediately. The PC must not be used until given permission from the IT Help Desk. A sign must be placed on the PC to warn other users. Any disks and USB memory sticks that have been used on the suspected infected PC should be gathered and not used.

6.7 Appropriate Use

- Employees must not install any personal accessories on company equipment.
- Employees must not install or connect any personal USB port replicators on the PC.
- Employees must not charge or connect USB electronic cigarettes on the PC.
- Employees must not charge or connect mobile phones, wireless chargers on the PC.
- Employees must not change the Windows default English language on the PC.

6.8 Remote and Home Workers

- Laptops must be kept in a secure location when not in use.
- Laptops must not be left unattended during the normal working day unless it is on company premises where there is good physical security at entrances to the building.
- When using portable equipment on the move, or outside of office hours, reasonable care should be taken to secure it.
- Data protection policy is enforced for remote and home working.
- Staff will need to ensure the screen is not overseen by third-party or captured by third-party premises CCTV camera.

6.9 Mobile Phones and Tablets

- Employees issued with company Mobile phones and Tablets are responsible for safekeeping and security.
- Security password and pin protection must be used where available to protect the mobile device and any stored data.
- Company mobile phones must not be left unlocked when unattended. Non-staff, including friends, family and children, must not be permitted to use company mobile phones.
- Employees whose mobile device is lost or stolen must immediately notify the IT department, who will be responsible for notifying the telephone company. In the event of the loss being detected outside normal business hours, the user should immediately notify the IT helpdesk by sending an email to itsupport@peoplesafe.co.uk , to ensure that call-barring is activated, thus minimising the Company's exposure for call costs.
- Personal mobile devices must not be connected to company PCs for charging, copying or synching.

6.10 Acceptable Use

- Users must comply with all applicable laws and adhere to the IT Cyber Security policy.
- The electronic resources must be used for business purpose.
- Users must respect the rights, privacy and property of others.
- Users must adhere to the confidentiality rules governing the use of passwords (as per password policy) and accounts, details of which must not be shared.
- The company network must only be used for work. Access to other networks, any exploits against such networks will be regarded as an unacceptable use of the company network.

6.11 Disposal of Media

- All computer equipment or digital media due for disposal must be treated as if it contained restricted information.
- If the computer is to be recycled, a secure method of data deletion shall be used before the unit is redeployed.
- Users must contact the IT department for disposal of company-owned computer equipment or media is required.
- Digital information may only be destroyed by the IT department or assigned third party provider.
- Computers must be securely wiped – Secure erase, DoD, prior to disposal.

6.12 Physical Media Transfer

Prior to routing physical media containing confidential or personal data, employees should:

- Identify the individual responsible for receipt of the physical media.
- Contact the recipient to confirm date/time of transport.
- Request written confirmation of receipt from the recipient.

6.13 Bring-Your-Own-Device

- The company does not allow the use of, or connection of, personal electronic devices to the corporate data network, IT systems or infrastructure.
- Internet fair usage on personal devices is acceptable on the Guest Wi-Fi only.
- Personal mobile devices are allowed to access the corporate M365 platform via the company's MDM (Mobile Device Management) solution.

7. Cloud Computing Controls

7.1 Cloud Security

This relates to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

- Use of cloud computing services for work purposes must be formally authorized by the IT department. The IT department will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the IT department.
- The use of such services must comply with Company IT Cyber Security policy.
- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the company.
- The IT department and DPO decides what data may or may not be stored in the Cloud.
- Personal cloud services accounts must not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

8. E-mail Controls

8.1 Email Security

- All emails are monitored, scanned and checked for spam, viruses and phishing by using a combination of M365 and Bitdefender security systems.

8.2 Appropriate Use

- Employees are to only use the company email for business communication and should not use it for non-work-related matters.
- Employees must take care when forwarding messages and consider if the recipient of their email requires the full content of the email or not, paying particular care when forwarding personal or sensitive data and when corresponding with external parties.
- Employees must not alter the text, or content of any received messages in a way that would be misleading or non-factual, including when forwarding them to others. Similarly, individuals must not assume that a forwarded message is a match of what was originally authored.
- Employees must not appear anonymous when sending e-mail.
- All emails should be finished with an email signature that includes the employee's name, job title and contact details and that complies with the company standard.
- Employees must not send or forward or share with colleagues by any other means any abusive, threatening, defamatory or obscene messages.
- Employees must take care with any suspected malicious or nuisance e-mails received (e.g., chain e-mail, hoax and spam e-mails) and delete them. If any suspicious e-mails are received, it should be reported to the IT Help Desk.
- Employees must never open attachments to an email of unknown origin as they may contain viruses and other malware.
- Employees must not open links to any suspected or phishing emails.
- Employees must not enter their username and password on any web links received by email.
- Employees emails may be accessed by colleagues to cover work.
- Under no circumstance should an employee connect or attempt to connect personal electronic devices to the company's corporate network or IT systems.

8.3 Mailbox Restrictions and Compliance

- Employee standard mailbox size is 50 GB. Once the mailbox limit is reached, the employee will not be able to send or receive any further mail and therefore housekeeping must be planned well in advance of reaching the email quota limit.
- All emails are stored and archived for a period of 7 years for compliance.

8.4 Calendars

- Employees are required to keep their calendars up to date.
- Employees are recommended to consider sending attachments or confidential messages by email, rather than include them in an Outlook appointment.

8.5 E-mail Disclaimer

The company publishes its professional intent in a disclaimer and any employees' email that is sent from the company email system to any external address will automatically have the disclaimer attached. The current disclaimer reads as follows:

> *"Peoplesafe is the trading name of Skyguard Limited, Guardian 24 Limited and Rocksure Systems Limited (together with "Peoplesafe"). This communication contains information which may be confidential, personal and/or privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any distribution, forwarding, copying or use of this communication or the information in it is strictly prohibited. Any personal views expressed in this e-mail are those of the individual sender and Peoplesafe does not endorse or accept responsibility for them. Prior to taking any action based upon this email message, you should seek appropriate confirmation of its authenticity. Skyguard Limited is a limited company registered in England and Wales, registered number: 4107459. Rocksure Systems Limited is a limited company registered in England and Wales, registered number: 5292192. Peoplesafe's registered office: Emerald House, East Street, Epsom, Surrey KT17 1HS. Guardian 24 Limited is a limited company registered in Northern Ireland, registered number: NI035286. Guardian 24 Limited's registered office: The Mount Business Centre, 2 Woodstock Link, Belfast, BT6 8DD."*

9. Internet Controls

9.1 Downloading of Information Resources

- Employees must not download non-work-related information from the internet. To reduce the likelihood of a virus infection, individuals must take care to ensure that the files are from a trustworthy source.
- Employees requiring any new software, including any plug-ins, must make a formal request to the IT Help Desk.
- Software must not be downloaded and/or installed on the PC.
- Graphical, audio and video files may be downloaded and stored on company's network for business use only.
- Employees are reminded that copyright laws apply to the internet and care must be taken should there be a need to re-use any information (including images) in any company's work.

9.2 Uploading of Content

- Employees who are responsible for uploading data / information to the internet must ensure that the information being uploaded is suitable to upload, and not official-sensitive.

9.3 Internet and Website Filter

- To protect employees and the company from an unregulated internet, we operate a "barred" list of known Websites that contain unacceptable content or represent unacceptable activity. Cisco web content filtering supplies the list and is automatically updated daily.
- All internet traffic is monitored and checked against Advance Malware Protection system for viruses and malicious software.
- Employees must not attempt to by-pass company's internet filtering system.
- Employees who encounter a commonly used business site which is blocked and have genuine business reasons for accessing that site frequently may contact the IT Help Desk to request access to the site.
- The company reserves the right to monitor employees use of all email, internet and business systems to ensure that the policies are properly observed.

10. Wireless Controls

10.1 Wi-Fi Security

- All the Wi-Fi Access points are centrally managed and monitored by the IT department.
- Corporate PCs, mobile devices and tablets are only allowed to connect to the corporate Wi-Fi where the authentication is done via the Radius server.
- A Guest Wi-Fi network is operated for visitors and third-party contractors only which maintains access to the internet over a separate VLAN.
- The passwords to access the Guest Wi-Fi network is available from the IT Helpdesk.

11. Employee Access Controls

11.1 New Employees

- Head of departments must notify the IT department by completing and submitting the IT New Starter form at least two weeks before the employee's start date.
- Employee login accounts are supplied to the Head of department and HR. The employee will be prompted to change the password on first login.
- A PC will be configured to allow the employee to use company email, web services and ERP.
- IT cyber security policy is provided and explained to all new employees including contractors during the IT induction process on the first day of start and no later than three working days.

The process can be found here New Starter Process Map

11.2 Staff Screening

- A good control covers background verification and competence checks on all candidates for employment.
- Must be carried out in accordance with the relevant laws, regulations and ethics.
- Must be proportional to the business requirements, the classification of the information accessed, and the perceived risks associated.

Security Screening Policy is found here.

11.3 Employees Leavers

- The HR department will advance notify the IT department in writing of employee leavers, which will carry the leave date.
- Line managers are to ensure that arrangements are in place for the move and caretaking of any data or incoming email.
- Accounts and emails of employee leavers will be de-activated after 5 pm on the employee's leave date (which will revoke all the access) unless otherwise requested.
- All employee leaver accounts will be deleted after 3 months of the leave date.
- Line managers and HR department must ensure all IT equipment is returned to the IT department on the leave date.
- All the leavers including contractors need to maintain integrity of information even after the termination.
- This policy is communicated during the employment period and during the employee exit meeting.

The process can be found here Leavers Process Map

11.4 Access to Program Source Code

- Access to source code is not allowed by default to any staff.
- A formal request is required by the Head of Software to allow access for the staff.
- Strict controls are in place to restrict access to program source code libraires.
- Designated personnel maintain access to the source code.
- Source codes are kept secure in a separate location other than the operational systems.
- Regular checks must be conducted by relevant tools to verify the integrity and change of the source code.

11.5 Maternity and Paternity Leave

- The HR department will notify the IT department to disable the user account.

11.6 Visitor and Guest Accounts

- The company does not supply guest accounts for its internal IT systems and does not allow the use of non-company owned equipment to connect to corporate wired networks on its premises. Access to the Guest Wi-Fi, web only VLAN is allowed, via an authorised guest login credentials.
- Visitors will be refused access to the Guest Wi-Fi, if any aspect of the proposed use is considered by the IT department to be a threat to the security of company IT systems.
- The IT department must be notified if third party contractors or consultants with non-company IT equipment will be on site.

12. Employee System Access Rights

12.1 Initial Login – Default Access

Access to business IT systems is dependent upon the login and password combination. Change of password is enforced every 90 days.

Employees default access:

- Personal File store.
- Print Services.
- Company Email.
- M365 services.
- Internet.
- MS Teams.

Users access permissions are reviewed regularly on a quarterly basis.

12.2 Additional System Access Authorization

Head of departments are to determine individual system access requirements or change in job role and submit these on the IT New Starter Form.

IT department will authorise access to:

- Secure and restricted file storage areas.
- ERP business and Finance System, different levels of access will need to be granted for different roles.
- The ability to remotely connect to the company IT systems and networks.

12.3 Privileged Access Rights

- Provided as deemed necessary to carry out the individual's job role.
- The competence of users with privileged access rights is reviewed regularly on a monthly basis by the head of departments and IT team.
- No privileged access shall be granted without verifying the competency.

12.4 Management of Secret Authentication Information

- The allocation of secret authentication information is controlled through a formal management process.
- Line managers need to send written consent to the IT team for approval and access provision.
- Temporary secret authentication information must be given to the users in a secure manner.
- The user is given controlled and monitored access.
- The access is reviewed regularly and revoked, if required due to termination or change of role.

13. Clear Desk and Clear Screen

To improve the security and protect confidentiality of information, the company adopts a clear desk policy for papers and removable storage media and clear screen policy for information processing facilities. This is to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when areas are left unattended.

13.1 Clear Desk

Any material left exposed (e.g. on a desk, printer or cupboard top) is more susceptible to damage, disclosure or theft, particularly outside of office hours.

- Lock sensitive documents, paper and computer media out of sight in drawers or filing cabinets when not in use.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information must be erased.

13.2 Clear Screen

- Computers must not be left logged on when unattended and must be protected by screen lock.
- Printers must not be left logged on when unattended and must be logged off.

14. Cryptography & Encryption

- All users must ensure all assigned encryption passwords are kept confidential and not shared.
- All users must ensure encryption passwords are not written down on the encrypted device.

Cryptography shall be considered in the following scenarios:

- Laptops and Mobile devices.
- Authorised use of removable media such as USB memory sticks.
- Where classified data is transmitted across communications lines e.g., over the Internet.

14.1 Encryption Strength

- The method of encryption for the company devices is whole disk encryption. Based on the data protection risk assessment and wherever applicable the company would use CCTM certified, and FIPS-140-2 validated (e.g., AES128/256 bit) technology for encrypting confidential and other sensitive data.
- Cryptographic controls should be used in compliance with all relevant agreements, legislation, and regulations.
- Restrictions on import or export of computer hardware or software used to perform cryptographic functions or are designed to have cryptographic functions added.
- Restrictions on the use of encryption, especially in foreign countries.
- Methods of access to encrypted information used by the countries' authorities.
- Legal advice should be sought to ensure compliance before encrypted information or cryptographic controls are moved across jurisdictional borders.

14.2 Data at rest

The company desktop computers are accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed.

- Wherever possible confidential data at rest on computer systems owned by and located with identified users should be protected by port blocking via group access policy.
- Wherever possible confidential data at rest on computer systems owned by and located with identified users should be protected by encryption, Firewalls with strict access controls or an access control matrix that authenticate the identity of those individuals accessing the sensitive data.
- Password protection should be used by identified users in combination with all controls including encryption.
- Computer hard drives or other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure in accordance with restricted-data disposal policy guidelines.

14.3 Portable Devices

- All identified laptops must have approved device encryption software installed and the hard disk must be fully encrypted at all times. It is the user's responsibility to respond to any error messages and immediately report issues to IT Support, thereby ensuring the encryption mechanism is operating correctly.
- Confidential information stored on portable devices such as laptops must be encrypted using products and/or methods approved by the company authorized person.
- Portable devices such as laptops must not be used for the long-term storage of any confidential information.

14.4 Removable Media, Storage and USB memory stick

- Where it is necessary, authorized removable media including, and USB drives that contain confidential information must be encrypted.

14.5 Transmission Security

- Confidential information transmitted as an email message must be encrypted for identified and agreed recipient(s). Email encryption should be agreed in writing with recipient for transmitting encryption signatures.
- A dedicated transmission mechanism should be in place to share the files securely outside the network.
- Transmitting unencrypted confidential information using web email programs is not allowed.
- Wireless (Wi-Fi) transmissions that are used to access portable computing devices or internal networks must be encrypted using the IEEE 802.11i (WPA2) or better.

14.6 Encryption Key Management

- Effective key management is crucial for ensuring the security of any encryption system.
- Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.
- Keys in storage and transit must be encrypted.
- Keys are securely maintained in the company's password safe.

15. Infrastructure Access Controls

15.1 Infrastructure Access and Controls

- Development, testing and maintenance of the network infrastructure is managed solely by the IT department.
- External contractors to provide IT services or require access to IT systems must provide a copy of their IT Cyber security policy and will need to be authorised by the IT department.
- External contractors and internal employees, carrying out work on the infrastructure, will operate under the direction of the IT department.
- Contractors and internal employees providing new systems that will connect to the infrastructure and will transmit data over the infrastructure will discuss requirements and agree all stages of work with the IT department.
- External & Internal penetration tests are carried out annually by a third-party for auditing and cyber security and cyber security accreditations.

16. Security Incident Reporting

16.1 Incident

If an employee suspects that an IT related security incident has occurred or will occur, they should report it immediately to the IT department by sending an email to itsupport@peoplesafe.co.uk

- Any occurrence of a compromised user account.
- Any occurrence of a server infected with malware.
- Three or more simultaneous occurrences of Bitdefender notification infected with malware.
- Any other instance of malware or suspected intrusion that seems abnormal.

16.2 Reporting

- Information Security Incidents must be reported as soon as possible to itsupport@peoplesafe.co.uk or by calling on 020 8786 3366.
- Loss of any piece of IT equipment (computer, laptop, mobile phone, USB storage device, etc), is classed as a security incident and must be reported immediately.

16.3 Response

- IT department maintains policies and procedures to assist staff to prevent attacks and identify potential security incidents.
- IT sends out regular emails to keep staff up to date pertaining to the latest cyber security threats.
- If a cyber security event has been detected, the affected system is disconnected & user account is disabled so that it is completely isolated from the network.
- The threat is eliminated by removing malicious activity or restoring the system from backup, and the user account credentials are reset.
- Communication is sent out to users to ensure no other user has experienced the same threat.
- Required action is taken to ensure that the origin of the threat is blocked.

16.4 Management Procedure

- Follow the cyber security framework – identify, protect, detect, respond and recover.
- Deal with the incident immediately.
- Conduct regular meetings with the relevant teams and DPO.
- Notify the relevant parties via phone & email.

17. Incident Management

The company takes the threat of security breaches very seriously and is committed to educating the users about the imminent threat of a data breach.

17.1 Preparation

- Perform a risk assessment
- Identify confidential and sensitive assets.
- Define critical incidents the IT security team should prioritise.
- Setup an Incident Response Team.

17.2 Identification

- Monitor and detect anomalies in the IT systems.
- Check if the anomalies or deviations qualify as major security incidents.
- If an incident is discovered, source for additional evidence, confirm its type and severity.
- Document the findings.

17.3 Containment

- Implement short-term containment such as isolating the attack vector or compromised network or systems.
- Prioritize long-term containment to include temporary fixes to ensure the 24/7 running of systems and networks while rebuilding a clean system and network.

17.4 Eradication

- Eliminate viruses and malware from all systems and networks.
- Find out the root cause of the threat.
- Establish proactive actions to exterminate similar threats in the future.
- If the threat is caused by weak authentication, patch with strong authentication.

17.5 Recovery

- Restore all affected and patched systems online.
- Test, verify, and monitor to ensure that the systems and networks are working optimally.

17.6 Lessons Learned

- Perform a retrospective session not later than two weeks from when the incidents occur.
- Document the entire incident, investigate the security incident further, appraise what was done during containment, and understand if the process can be improved in the future when an incident occurs.

18. Information Security Review

- The organisation's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.
- The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained.
- Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Information systems is regularly reviewed for compliance with the company's IS policies and standards. Technical compliance should be reviewed by an experienced system engineer; if penetration tests or vulnerability assessments are used, caution should be exercised - such tests should be planned, documented and repeatable. Any technical compliance review should only be carried out by competent, authorized persons or under the supervision of such persons.

19. Asset Management

Computer systems, network hardware and software which are used to process data are considered as information assets. The main categories of information asset are:

- Information: Databases, system documentation, procedures, media and data.
- Software: Application programs, systems, development tools and utilities.
- Physical: Infrastructure used for data processing.
- Services: Computing and communications, power, air conditioning used in the business premise.
- People: Qualifications, skills and experience in the use of information systems.

19.1 Asset Register

The IT systems and asset register must be kept up to date for compliance and audits. The IT team is responsible to ensure that register is kept up to date.

All the assets in the register are owned and licensed by the company.

19.2 Asset Owner

The ownership of all type of assets are delegated to the staff member to whom the asset has been assigned. The overall ownership of the asset is maintained by the IT team.

20. Licensing and Procurement Controls

20.1 Licensing Compliance & Software Asset Management (SAM)

- The IT department is responsible for software licensing compliance for all company IT equipment.
- Administrative records are retained, recording when licenses are due for renewal, which licenses are site-wide, how many single or concurrent licenses are held/deployed. The company has an auditing tool that manages concurrency, software controls, audit and monitoring.

20.2 Software Copyright and Software Theft

- Software auditing detects unauthorised software download patterns and reports will instigate an investigation where it is found that employees are downloading unauthorised software or bringing in software that is not authorised for business use.
- The use of software key generators or license key crackers is strictly forbidden, disciplinary action will be taken if any employee is found in possession or found using these software tools.

20.3 Procurement

No IT hardware, software, subscriptions, licenses, mobile devices and peripherals shall be purchased without the consultation and authorisation of the IT department.

21. Data Protection Compliance

- Changes in the law governing Data Protection as well as changes in technology have outlined new areas of risk – particularly where remote work is undertaken, where increasingly portable appliances are used, where portable company equipment is removed from the office environment for reasons of travel or customer/supplier visits. This section of the IT Security policy summarises the controls that the company exerts to protect its data.
- It is a breach of policy to remove screen-dumps or output files that contain employees' personal and client data records from the company – whether by transmission e.g. email or file transfer, or by portable storage device e.g. PDAs, Zip drives, CDs and USB sticks. Users who do so will be disciplined, and may be subject to legal action under the Data Protection Act/General Data Protection Regulations

21.1 Data Protection - Remote Working

- The company allows external access to company data stored on internal systems, only by approval and only by remote VPN access using company equipment.
- All data referring to any employee's personal records must be accessed and stored on company servers and not on local devices or removable media.

21.2 Visibility of Personal Data within Company Premises

- All users must logout or lock the computer equipment before leaving their desk.
- Company computer equipment will auto-lock after a period of inactivity, thus removing data display on the monitor.

21.3 Remote Working and Offsite Equipment

- Data that falls into the category of "Company Business Data" E.g., business files or deemed the company's intellectual property but is not sensitive personal data, should be primarily stored on a company's file storage areas and accessed from there. It is accepted that this data may be transported on a company laptop from time to time for offline working, but company business data should never be loaded or stored on personal home computers or laptops or accessed by any device that is not protected by the company anti-virus or digital security systems.
- Employee are advised to save prime copies of their data on their company allocated file storage. Employees are advised that the company is not responsible for that data in any other storage location (E.g., when saved to local drives, usb sticks or removable hard drives).

21.4 Portability of Company Data

- The company's personal data record kept on employees & customers must not be ported on USB memory sticks, PDAs, removable media, discs.

21.5 Enforcement - User Training

- Users are instructed during the Employee Induction Process of their responsibilities for securing Company and Personal Data files and records and of the disciplinary procedure should the policy be breached.

22. Classification of Information

All company information and third-party information is categorized as per one of the below categories:

22.1 Unclassified Public

Information is not confidential and can be made public without any implications for the company.

- Product brochures widely distributed.
- Information widely available in the public domain, including available on web site areas.
- Financial reports required by regulatory authorities.
- Newsletters for external transmission.

22.2 Proprietary

Information is restricted to approved internal access and protected from external access. Unauthorized access could influence the company's operational effectiveness, financial loss, significant gain to a competitor, or cause a major drop in customer confidence.

- Passwords and information on corporate security procedures.
- Know-how used to process client information.
- Standard Operating Procedures used in all parts of the company's business.
- All company-developed software code.

22.3 Client Confidential Data

Information received from clients for data processing by the company. The original copy of such information must not be changed in any way without written permission from the client.

- Client media
- Client personal information of any form.
- Electronic transmissions from clients

22.4 Company Confidential Data

Information collected and used by the company to employ people, client orders and manage all aspects of corporate finance. Access to this information is very restricted within the company.

- Salaries and other personnel data.
- Accounting data and internal financial reports.
- Confidential customer business data and confidential contracts.
- Non-disclosure agreements with clients & vendors.
- Company business plans.
- Securely stored on the company's cloud systems.
- Designated personnel maintain access.

22.5 Restricted Data

Restricted data is a combined category of the confidential data which can be formed from Proprietary, Client & Company confidential classification.

- Sensitive personal data.
- Personal data.
- Commercially sensitive data.

22.6 Labelling of Information

- Unclassified Public: Peoplesafe do not use any form of information classification labelling for this category.
- Proprietary: Peoplesafe use label for pricing tool, corporate information, and procedure. Use of label is granted through approval of the management team. Only appropriate users are added to the access list of such information. Peoplesafe maintains paperless documentation, labels are added to all required documents and visible on top of the document with permission message:

- Designated IT staff are only allowed to give or remove access permissions.
- Other classified information is labelled as per the category. Such as client data – Sensitive label, Staff's personal data – Sensitive label, company business plan – Private & Confidential label, for other restricted data – Legally Privileged & Confidential label.

The company has established procedures to protect all the classified information as per the below table:

Category	Internal (Proprietary, Staff sensitive, Business Plan)	Restricted (Sensitive personal, commercial)	Confidential (Staff, Company, Customer)
Paper Records	N/A	N/A	N/A
Digital Files (Server, PC)	Must not print, if printed should be disposed off through secured shredder. PC protection policy applies to all the internal data. Information classification label is attached as per the category.	Must not print, PC protection policy applies to all the internal data. Information classification label is attached as per the category.	Must not print, PC protection policy applies to all the internal data. Information classification label is attached as per the category.
Removable Devices	Not Granted without explicit permission	Not Granted without explicit permission	Not Granted without explicit permission
Email	Information classification label must be attached centrally or by the user as per the classified information type	Information classification label must be attached centrally or by the user as per the classified information type	Information classification label must be attached centrally or by the user as per the classified information type

22.7 Agreements Information Transfer

- Information sharing between Peoplesafe and any other third party if required is controlled by the contractual agreement.
- Only certain types of data sharing are permitted when required.
- All the data must be encrypted with security label and shared with the target person only.
- Personal data sharing is not permitted under any circumstances unless it is for legal purposes.
- Data subject consent is required for sharing personal data.
- All the policies of GDPR act 2018 are followed by both the parties.

The data transfer agreement is found here Data Transfer Agreement

23. Operations Management

23.1 Change Control – Software

An effective change control procedure is in place to cover all changes to the IT systems and Software development.

All change requests are logged on the system as per the below categories:

- Major
- Standard
- Minor
- Emergency

23.1.1 Version Control and Patching

The company agrees updates and patches of its operating system and application platforms via a strategic process, managed by the IT department:

- Ensures coherence across the installed user base.
- Supplies a platform that is compatible with and has been tested to support key company business applications and backbone systems.
- It is company policy that no individual or department changes the operating system base or the application system base without authorisation of the IT department.

23.2. Stages of process

23.2.1 Proposal for Software Upgrade

- The proposal may arise in user groups, functional strategic management processes or from users or providers.

23.2.2 Technical Consultation & Acceptance Testing

- The proposal is examined by the Technology CAB (Change Advisory Board) who will examine technical feasibility, compatibility, the need for technical change, test results of the version proposed and assess the impact of the process.

23.2.3 Cost and Licensing Cover

- Licensing status and whether there are any costs associated with the proposal will be examined by the budget holder and IT department.

23.2.4 Software Procurement

- The software is procured subject to the company Financial Regulations.

23.2.6 Communication and Preparation

- The project is communicated to key users. A project team is set up and an implementation, training and support plan prepared.

23.3 Technical Communication Control

- The IT department issues instructions, warnings or advice to the users and at times will require users to take emergency preventative action.

23.4 Management of Technical Vulnerabilities

- Centralized IT security systems proactively scans networks and IT systems for security vulnerabilities on a daily basis. If a vulnerability is found, the IT department receives immediate alerts & notifications.
- Full vulnerability scan is carried out automatically on a weekly basis.
- Managed through the risk assessment process and actions resulting from event logging.
- Penetration tests are conducted annually, and a clear incident breach management policy is defined in the IT Cyber Security policy
- Weekly operational meetings are held.

23.5 Audit Controls

- The company has an auditing tool that manages concurrency, software controls, audit and logs monitoring.
- Audit activities involving checks on operational systems are planned to minimise the risk of disruption to business process.
- Any risk is noted in the risk register and communication is sent out to the business.

23.6 Event Logging

- Effective systems are in place for confidentiality audit and event logging.
- Event logs record user activities, exceptions, and information security events
- Logs are produced and maintained for 90 days to assist in investigations and access control monitoring.
- Various OSS and BSS have their own mechanism to record the audit logs.
- Logs are reviewed on a weekly basis and alerts are set to trigger automatically if any unauthorised event is detected.

23.7 Capacity Planning

- Capacity demands are monitored to ensure that adequate processing power and storage are available to meet future demands.
- Company monitors systems networks and information processing facilities via various proactive monitoring tools.
- Dashboards, Alerts and notifications (emails) are set up to provide a real time OSS & BSS monitoring update.
- Continuous monitoring is performed to check the health of the systems via our monitoring tools. Alerts are triggered if any system performance is below a set threshold level.

23.8 Separation of Development, Testing and Operational Environments

- Development and operational software operate on different systems.
- Continuous Integration & Deployment pipeline in place which incorporates Dev and Test environments to be separate from the live system.
- Test platform is used for training.

23.9 Information Backup

- All the servers' backups are done daily and are verified to ensure it is consistent and a monthly restore exercise is performed to test the data integrity of the backups.
- The offsite backups are done daily

23.10 Clock Synchronization

- All the workstations' clocks are synchronised with the internet time server

23.11 Operational Software Control (Hardening and Patching)

- All operating system, software, hypervisor, and firmware are always kept up to date to safeguard against any security vulnerabilities.
- Security updates & patches are tested thoroughly in the test environment before being deployed to the live environment. A system snapshot and backup of the config is maintained to ensure IT can roll back if required.
- Windows security updates & patches are automatically deployed to the workstations every 2 weeks to protect against cyber threats. These are tested before being deployed to the workstations.
- All unnecessary software, system services, protocols, ports, and drivers are removed.
- Domain-based Active Directory server-based group policies are applied.
- When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.

24. Software Development Security

24.1 Secure Development

- All software development must include security and privacy in the design phase.
- Evidence of threat modelling must be collected for all exposed input.
- All software must be tested for vulnerabilities before deployed into production.
- Vulnerabilities must be addressed as per the Vulnerability Standard.
- Only approved libraries may be used in software development.
- Only approved languages may be used in software development.
- Software must be designed to be resilient.
- Software must be designed to maintain the confidentiality of all data available and collected.
- Software must be deigned to be available regardless of load and remain functional while under an attack.
- Software must be designed to preserve the authenticity and integrity of all data collected and referenced.
- All application functionalities must pass an authorization check before being utilized.
- Software must be designed so that no input is written directly into any back-end system including databases.
- No software may use routines or algorithms not internally developed without review, testing, and approval.
- All externally developed routines, algorithms, or libraries in use must be properly licensed for use.

24.2 Software Packages Changes

Modifications to software packages is not encouraged once it is in the live environment. Changes to software packages must follow the below steps:

- Only dedicated software developers can access the source code upon required authorisation.
- Changes to the source code is tested in a secure test environment followed by UAT.
- Security checks are conducted following the change.

24.3 Secure Systems Engineering

- Security must be designed into all architecture layers to balance security with accessibility.
- New technology must be analysed for security risks.
- Design must be reviewed against known attack patterns.
- Principles must be reviewed to ensure effectiveness to enhance standards of security within the engineering process.
- Principles must be reviewed to ensure it is up to date against any new potential threats.

24.4 Secure Development

The secure development lifecycle can be found here Secure Development Lifecycle

24.5 Outsourced Development

All the development works are done in-house. Any outsourced development if required must be authorized and the third-party must agree and sign the IT Cyber security policy.

24.6 System Security and Acceptance

The secure development lifecycle can be found here Secure Development Lifecycle

24.7 Test Data Protection

- Test data must be selected carefully, protected and controlled.
- Test data must be generic with no relation to the live system data.
- Live data used for testing must be anonymised and securely deleted when testing is complete.
- Use of live data must be pre-authorised, logged and monitored.

25. Information Security Requirements

- Any new system development or change to existing systems, the business requirements for security controls must be carried out by doing a risk assessment.
- Risk assessment must be done prior to the selection or commencement of the development of a solution.
- Security considerations must be taken into consideration from the earliest possible opportunity to ensure that the correct requirements are identified before solution selection.

Information security template is utilised to assess the security risks which is attached here Information Security Template - Project

26. Risk Management

IT department regularly carries out risk management and processes to safeguard against:

- User accounts cannot be accessed
- Customers receive spam from an employee business account
- Passwords no longer work
- Data is missing or altered
- Hard drive runs out of disk space
- System constantly use draining memory
- Malicious website links
- Malicious links embedded in emails
- Malicious attachments received via email
- Phishing websites

Security audit processes in place to ensure:

- All users are using complex passwords.
- Users are not using browser password or credential savers.
- Passwords are not written down or given to other employees or any other person under any circumstances.
- Passwords must be a minimum of 7 case sensitive characters and should be a combination of upper/lower/numeric and special characters such as #@?!$& etc. Passwords must include at least three different character types, or they will not be accepted.
- Change of passwords is enforced every 90 days.
- User accounts will be locked after 4 invalid login attempts.
- User accounts are disabled for leavers on the leaving day.
- Users' computers are locked when away from their desk.
- Users do not charge or connect USB electronic cigarettes on the PC.
- Users do not charge or connect mobile phones, wireless chargers on the PC.
- Remote access is only allowed for limited employees through the VPN, all activities are monitored.
- Daily check procedures in place to ensure backups are up to date.
- Access to network cabinets and datacenter areas are restricted to named IT personnel.
- Access to mission critical systems is restricted to named IT personnel.

27. Business Continuity Management

Information security continuity is embedded in the organization's business continuity management systems. The company determines its requirements for information security and the continuity of information security management in adverse situations, e.g., during a crisis or disaster.

Disaster recovery system is tested every 6 months.

Please refer to the Business Continuity Plan

28. Relevant Authority Contacts

Relevant authority contacts are kept up to date with regular checks from relevant authority website i.e., police, ICO, service providers. The contact is to be made via email and telephone where necessary by the dedicated team member from relevant department. Contact is made if there is any service downtime or other emergency. Relevant data with the respective authority is shared.

The contact details are found here

29. Contact Special Interest Groups

Membership with specialist forums and professional associations are controlled by prior authorization from the IT and Compliance team. No one is allowed to be a member of such associations if there is no relevance and necessity of doing so. The Membership login details are kept secure in the password safe which is maintained securely which helps delete such membership if required.

30. Information Security Project Management

A template framework is adhered to which integrates with the project management process to assure that the information security is maintained throughout the project implementation. All the staff involved in any project must complete and abide by the framework during the project work. The template is found here Information Security Template - Project

31. Supplier Relationship

- The company depends on strategic suppliers, several of whom are critical to the service.
- The company may suffer poor performance and financial loses if a vendor is not selected properly by following a due-diligence process.
- Prior to signing a contract with a supplier, it is essential to carry out due diligence to check that the supplier can meet their obligations to deliver, either based on the content of a contract or against their marketed claims.
- All relevant information security requirements, SLA are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the company's information taking into account the criticality of information.
- Awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information are in place.
- The company regularly monitors, reviews and audit supplier service delivery.

A list of approved suppliers is maintained on the company's QMS system.

32. Identification of Applicable Legislation and Contractual requirements

A good control describes how all relevant legislative statutory, regulatory, contractual requirements, and the organisation's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organisation.

32.1 List of Applicable Legislation and Contractual Requirements

32.1.1 List of Applicable Legislation

- Sale and Supply of Goods Act (HMSO 1994)
- Intellectual Property Act 2014
- Data Protection Act 2018
- Consumer Rights Act 2015
- Malicious Communications Act 1988
- Freedom of Information Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications)
- Regulations 2000

32.1.2 Contractual requirements

- Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
- Any new legislation / amendments, the relevant document shall be identified, and action would be initiated by the management through internal communication records to all concerned.
- Any changes to be incorporated at organisation level or changes due to changes in legal and other requirements regarding the existing work practice the same shall be decided and communicated to the interested party.
- Both parties have obligations to fulfil the contractual requirements.

33. Breach of Policy

The company expects all employees to always follow this policy and those who do not abide by this policy and cause security breaches may face disciplinary action.

Employees who attempt to sabotage the company provision will be disciplined and depending upon the severity of the attempt/incident, dismissed, in line with the company's Disciplinary Procedure.

33.1 Misuse & Violations

Any employee found to be misusing the communications equipment and systems provided by the company will be treated in line with the usual disciplinary procedure.

Violations of this IT Cyber Security policy may include but are not limited to any act that:

- Exposes the company to actual or potential monetary loss through the compromise of data security or damage or loss of computer equipment.
- Involves covert recording of ad-hoc conversations via the company or personal mobile, hand-held device or any type of recording device, the use of data for illicit purposes, which may include violation of any law, regulation or reporting requirement of any law enforcement or government body.
- Sharing of company information with any external or internal entity who are not expected to access or view the information.

33.2 Penalties for non-Compliance

The viewing, transmission, downloading, uploading or accessing any of the following material using the company communications equipment and systems will amount to gross misconduct:

- Any material which is pornographic, sexist, racist, homophobic, paedophilic or any other discriminatory or otherwise offensive.
- Illegal or criminal material, including material which breaches copyright or any other information protection right.
- Any material which has the object or effect of causing harassment to the recipient.
- Any material which the employee is aware is of confidential or restricted information and which they are not authorised to deal with.
- Any website which the company has blocked access to from the company communications equipment and systems.
- Disclosing confidential or sensitive company/customer information with external entities, competitors are regarded as information security breach.

Non-compliance or violation of this IT cyber security policy shall be treated as willful misconduct and breach of information security and will result in action that may include, but not be limited to, the following:

- Suspension of employment.
- Termination of employment.
- Other disciplinary action.
- Civil and/or criminal prosecution.

34. Acknowledgment of Acceptance

I understand and sign to verify that I have read and accepted this policy IT-P01–IT Cyber Security. I understand and agree to comply with the IT Cyber Security Policy.

Name of Employee: ……

Job Title: ……

Department: ……

Date: ……

Signature of Employee: ……

Appendix 1: Summary of Legal Requirements

Computer Misuse Act (1990)

- Unauthorised access to computer material. Commonly referred to as hacking.

  Penalty: Up to six months in prison and/or a or up to a £5,000 fine

- Unauthorised access to computer materials with intent to commit a further crime. This refers to hacking a computer system to steal or destroy data (such as planting a virus).

  Penalty: Up to a five-year prison sentence and/or an unlimited fine

- Unauthorised modification of data. This refers to the modification or deletion of data and covers the introduction of malware or spyware onto a computer device (electronic vandalism and theft of information).

  Penalty: Up to a five-year prison sentence and/or an unlimited fine

- Making, supplying or obtaining anything which can be used in computer misuse offences

  Penalty: Up to a ten-year prison sentence and/or an unlimited fine

General Data Protection Regulation

The GDPR is a comprehensive regulation that unifies data protection in all EU countries. It will directly apply in all EU member states from 25th May 2018. The GDPR has a very broad territorial scope and will apply to any organisation that manages the personal data of individuals who are based in the EU, regardless of where the organisation is registered. Non-compliance leads to severe consequences. Fines may amount to a maximum of EUR 20 million, or 4% of global annual turnover. The GDPR requires organisations to implement reasonable data protection measures to protect the personal data of consumers and employees against data loss or exposure. To achieve that goal, the law regulates all areas related to data management and processing, from obtaining user consent to setting up company-wide data protection practices and handling data breach incidents.

Any Company data users must comply with the seven Data Protection Principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability