bluesource Information Security

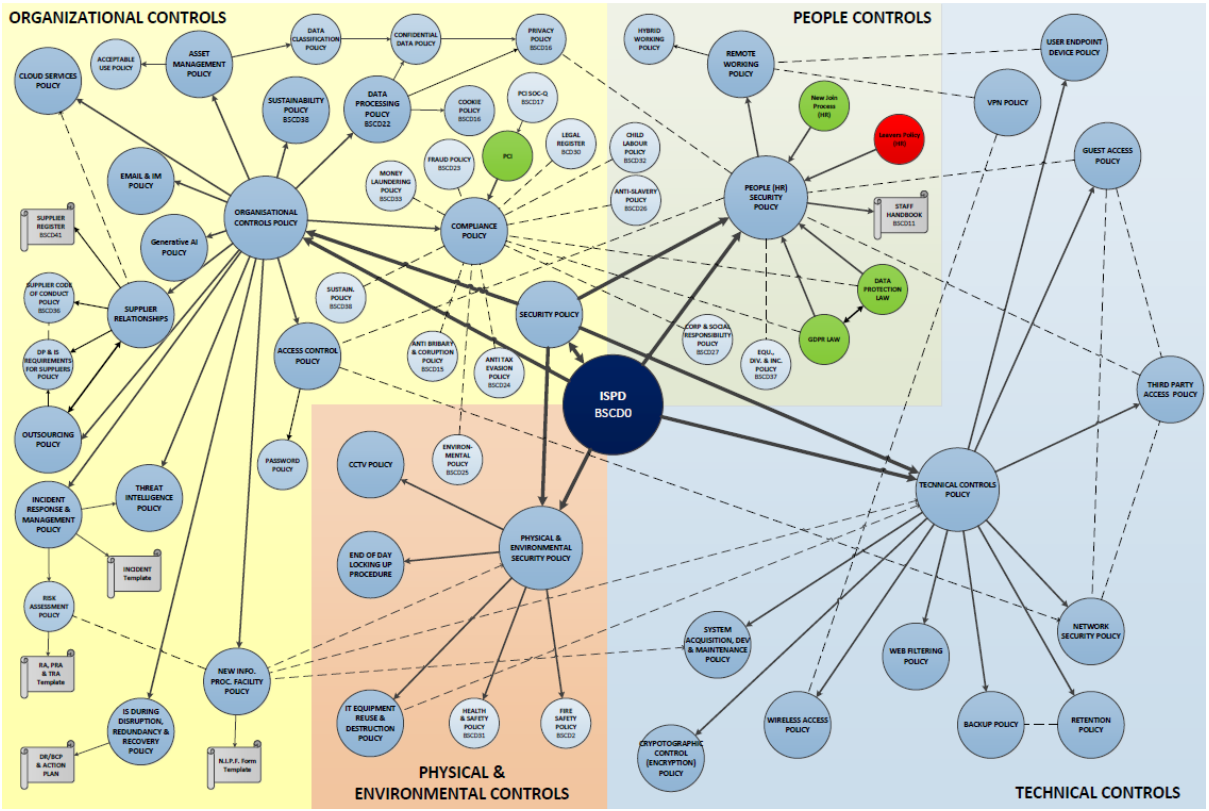
Information security, or "**IS**" as it is sometimes simply referred to as, is at the forefront of all that we do at bluesource (referred to later as the Company), not only to protect ourselves as a business but also to ensure we are providing a secure, safe environment in which to engage with our customers, partners, and employees. We aim to provide robust and secure, products and services, and consider information security by design, in all that we do.

The following information summarises our approach to information security and aims to provide confidence and instil trust in all that we do and help support our customer and partner journeys, whether existing or prospect.

bluesource protects its data in line with the requirements of applicable data protection legislation and is commensurate with the processing and level of associated risk. We are certified to ISO27001 and Cyber Essentials.

For more information on how we handle the data that we collect, please see our data processing and privacy policies.

Information Security Policy



bluesource maintains a comprehensive information security management system ("ISMS") and suite of information security policies based around and certified against the internationally recognised ISO27001 standard and utilising the ISO27002:2022 control set, broken down into key areas, including:

- Organisation Controls
  - Access Provisioning and Review
  - Asset management
  - Business Continuity and Disaster Recovery management
  - Incident management and response
  - Information Classification and Handling
  - Supplier relations
  - Vulnerability and Threat Management

- People Controls
  - Personnel Security and Security Awareness

- Physical and Environmental Controls

- Technical Controls
  - Application and system security
  - Cryptographic and encryption controls
  - Network security
  - Security monitoring

As part of our ISMS, we define management and employee responsibilities and acceptable use of information system resources. bluesource receives signed acknowledgment from employees indicating that they have read, understand, and agree to abide by its' policies, acceptable use, and rules of behaviour upon commencement of employment and receive ongoing training and assessment on a regular basis, on topics such as data protection and information security.

bluesource's policies and identified risks are regularly reviewed, at least annually, with revised versions published as necessary and held under version control.

Organisational Security

bluesource's Head of Operations, reporting to the Managing Director and Board, is responsible for the compliance and governance of the Company's ISMS and its certification to ISO27001.

They also perform the role of Data Protection Officer (DPO), chair the security team meetings, and lead an incident response team (IRT), comprised of senior individuals, including leaders from across the business, facilitating the appropriate executive engagement for security program oversight and risk management.

Information security roles and responsibilities are further defined within the Company with clear delineation of responsibilities and segregation of duties, with all employees having their key part to play.

bluesource maintains contact with relevant authorities and with special interest groups, such as CISA and NCSC, who can assist with the Company's threat intelligence activities.

Key operational security controls include:

- **Threat Intelligence** - To provide awareness of the Company's threat environment so that the appropriate mitigation actions can be taken, information relating to information security threats are collected and analysed to produce threat intelligence. The Company also has a process for addressing zero-day vulnerabilities that includes threat intelligence for visibility, scanning for assessment of threat, and emergency escalation provisions for remediation.

- **Information Security in project management** - To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout a project's lifecycle, relevant aspects of information security are integrated into project management.

- **Inventory of information and other associated assets** - To identify the Company's information and other associated assets to preserve information security (i.e., confidentiality, integrity, and availability), and assign appropriate ownership, the Company has developed and maintains inventories of applicable information and other associated assets. The Company's assets, including those entrusted to its care where applicable, are formally classified based upon sensitivity and criticality, and protection is driven accordingly by security policies and procedures.

- **Acceptable use of information and other associated assets** - To ensure information and other associated assets are appropriately protected, used, and handled, rules for the acceptable use and procedures for handling information and other associated assets are identified, documented, and implemented.

- **Return of assets** – To protect the Company's assets as part of the process of changing or terminating employment, contract or agreement, personal and other interested parties must return all the Company's assets in their possession upon termination of their employment, contract, or agreement, or where they no longer require such asset.

- **Classification of information** - To ensure that the protection needs of information are identified and understood, in accordance with its importance, information must be classified according to the information security needs of the Company, based on confidentiality, integrity and availability, and the requirements of any relevant interested party/ies. Relevant data classification levels are applied to any customer data it processes. Where bluesource or one of its service partners host customers' data, it does not inspect or monitor the customers' data and has no ability to understand how any data may have been classified by individual customers. Customer data is handled according to its policies for all customer data, with the customers remaining the data controller (i.e., data owner) for all data they store in such hosted instance and should therefore apply access controls according to their data classification policies.

- **Labelling of information** - To facilitate the communication of classification of information and support automation of information processing and management, the Company has developed and implemented an appropriate set of procedures for information labelling, in accordance with the information classification scheme adopted, and have linked this to sensitivity flagging control, within its DLP system. All confidential information is labelled as such and controlled through Office 365 sensitivity controls wherever possible, such as restricting information sharing and providing a basis for DLP protection.

- **Information transfer** - To maintain the security of information transferred within the Company and with any external interested party, information transfer rules, procedures, or agreements are in place for all types of transfer facilities within the Company and between the Company and other relevant parties.

- **Access Control** - To ensure authorised access and to prevent unauthorised access to information and other associated assets, the Company has put in place rules to control physical and logical access to information and other associated assets based on business and information security requirements.

- **Identity Management** - To allow for the unique identification of individuals and systems accessing the Company's information and other associated assets, and to enable appropriate assignment of access rights, the full lifecycle of identities is managed from creation through to termination.

- **Authentication information** - To ensure proper entity authentication and prevent failures of authentication processes, the allocation and management of authentication information is controlled by a management processes, including the advisory on handling authentication information.

- **Access Rights** - To ensure access to information and other associated assets is defined and authorised according to the business requirements of the Company, access rights to information and other associated assets are provisioned, reviewed, modified, and removed in accordance with the Company's "Access Control Policy". Access is on a "need-to-know" and "minimum rights" basis, with privileged identity management and "just-in-time" in place.

- **Information security in supplier relationships** - To maintain an agreed level of information security in supplier relationships, processes and procedures are defined and implemented to manage the information security risks associated with the use of supplier's products and services.

- **Information security in the ICT supply chain** - To maintain an agreed level of information security in supplier relationships, processes and procedures are defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

- **Monitoring, review, and change management of supplier services** - To maintain an agreed level of information security and service delivery in line with supplier agreements, the Company regularly monitors, reviews, evaluates and manages change in supplier information security practices and service delivery.

- **Information Security for Use of Cloud Services** - To specify and manage information security for the use of cloud services, the Company has established a process for the acquisition, use, management and exit from cloud services, in accordance with its information security requirements.

- **Information security incident management planning and preparation** - To maintain an agreed level of information security in supplier relationships, processes and procedures are defined and implemented to manage the information security risks associated with the use of supplier's products and services.

- **Assessment and decision on information security events** - Information security events are assessed at the earliest opportunity, to determine whether they should be classified as information security incidents by the Service Management Centre (SMC) in conjunction with the Head of Operations, to help identify the impact and extent of an incident.

- **Response to information security incidents** - To ensure efficient and effective response to information security incidents, they are responded to in accordance with documented procedures. The Company has a formalised incident response plan and associated procedures in case of an information security incident. The Incident Response Plan defines the responsibilities of key personnel and identifies processes and procedures for notification. Incident response personnel are trained, and execution of the incident response plan is tested periodically. An incident response team is responsible for providing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

- **Learning from information security incidents** - To reduce the likelihood or consequences of future incidents, the knowledge gained from information security incidents is used wherever possible to strengthen and improve the Company's ISMS and relevant controls.

- **Collection of evidence -** To ensure a consistent and effective management of evidence related to information security incidents, for the purposes of disciplinary and legal actions, the Company has established and implemented procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.

- **Information security during disruption -** To protect information and other associated assets during disruption, such as a DR event or other security incident, bluesource has planned how to maintain information security at an appropriate level during the disruption within its DR and BCP plans.

- **ICT readiness for business continuity -** To ensure the availability of the Company's information and other associated assets during a disruption, the Company has planned, implemented, maintains, and tests its ICT readiness based on its business continuity objectives and continuity requirements.

- **Legal, statutory, regulatory, and contractual requirements** - To ensure compliance with legal, statutory, and contractual requirements related to information security, these requirements are identified, documented, and kept up to date.

- **Intellectual Property rights** - To ensure compliance with legal, statutory, regulatory, and contractual requirements related to intellectual property rights and use of proprietary products, the Company has implemented appropriate procedures to protect intellectual property rights.

- **Protection of Records** - To ensure compliance with legal, statutory, regulatory, and contractual requirements as well as community or social expectations related to the protection and availability of records, records are protected from loss, destruction, falsification, unauthorised access, and unauthorised release.

- **Privacy and protection of personal identifiable information ("PII")** - To ensure compliance with legal, statutory, regulatory, and contractual requirements related to the information security aspects of the protection of PII, the Company has identified and meets the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements, such as and not limited to the Data Protection Act 2018 and GDPR. We apply a common set of data management principles to partner and customer data that we may process, handle, and store. We protect all data using appropriate physical, technical, and organizational security measures. The Company only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorised by consent in accordance with its privacy policy.

- **Independent review of information security** - To ensure the continuing suitability, adequacy, and effectiveness of bluesource's approach to managing information security, its approach to this and its implementation, including people, processes, and technologies, is reviewed independently at planned intervals, or when significant change occurs.

- **Compliance with policies, rules, and standards for information security** - To ensure the correct and secure operation of information processing facilities, operating procedures where necessary are documented and made available to personnel who need them, commensurate with the complexity of the processing and potential risk.

- **Documented operating procedures -** To ensure the correct and secure operation of information processing facilities, operating procedures where necessary are documented and made available to personnel who need them, commensurate with the complexity of the processing and potential risk.

People Security and Conduct

People are at the very heart of our business and are necessary to maintain the bluesource's reputation for high quality services and its standards, so getting the right people from the start is paramount.

Our employees and those working for us, on our behalf, are required to conduct themselves in a manner consistent with the Company's guidelines, including those regarding confidentiality, business ethics, and professional standards. All employees are required to sign confidentiality agreements within their contracts of employment and where non employed workers are used, such arrangements are made contractually within supply agreements.

Employees are provided with security training at the time of hire and on an ongoing annual basis. Security training covers a broad section of topics around security awareness (ISO27001 and the Company's ISMS), compliance (including data protection, DPA 2018 and GDPR) and privacy. In addition, Company employees are required to complete internal annual assessments based on the training.

Key people security controls to achieve this include:

- **Screening -** To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment, candidates are screened to ensure their suitability.

- **Terms and Conditions of employment** - To ensure personnel understand their information security responsibilities for the roles for which they are considered, contractual agreements cover applicable information security responsibilities.

- **Information security awareness, education, and training** - To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities, all employees and, where relevant, contractors receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

- **Disciplinary process** - To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation, a formal disciplinary process is in place and communicated to act against those who have committed an information security breach.

- **Responsibilities after termination or change of employment** - To protect the Company's interests as part of the process of changing or terminating employment or contracts, information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated, and enforced.

- **Confidentiality or non-disclosure agreements** - To maintain confidentiality of information accessible by personnel or external parties, requirements for confidentiality or non-disclosure agreements reflecting the Company's needs for the protection of information are identified, regularly reviewed, and documented.

- **Remote Working** - To ensure the security of information when personnel are working remotely, such as necessary for hybrid working, a policy and supporting security measures have been implemented to protect information accessed, processed, or stored outside the Company's premise/s.

- **Information security event reporting** - To support timely, consistent, and effective reporting of information security events that can be identified by personnel, such events are reported through appropriate management channels as quickly as possible. Similarly, any observed or suspected information security weaknesses in systems or services, are reported in the same way.

Physical and Environmental Security

Whilst bluesource utilises cloud based and SaaS services wherever possible, such as Microsoft Azure and Microsoft 365, etc., it has policies, procedures, and infrastructure in place to handle the physical and environmental security needed for its corporate office in London.

Guest access to its premise is controlled and a separate "Guest Wi-Fi" facility is in place to ensure connection to the corporate network is distinct.

The premise employs access, alarm, CCTV, and fire control systems.
Our information systems and infrastructure are hosted by world-class cloud providers, such as Microsoft, that are geographically dispersed and offer an equivalent or better level of security that we could aim to achieve ourselves.

Key physical and environmental security controls include:

- **Physical security perimeter** – To prevent unauthorised physical access, damage and interference to the Company's information and other associated assets, a security perimeter has been defined and put in place to protect areas that contain such assets.

- **Physical Entry** – To ensure only authorised physical access to the Company's information and other associated assets occurs, secure areas are protected by appropriate entry controls and access points.

- **Securing offices, rooms, and facilities** – To prevent unauthorised physical access, damage and interference to the Company's information and other associated assets in offices, rooms and facilities, physical security for offices, rooms and facilities is designed and implemented.

- **Physical Security Monitoring** – To detect and deter unauthorised physical access, the premises are continuously monitored for physical access.

- **Protecting against physical and environmental threats** – To prevent or reduce the consequences of events originating from physical and environmental threats (such as fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster), threats to infrastructure are considered and controls designed and implemented to reduce such risks.

- **Working in secure areas** – To protect information and other associated assets in secure areas from damage and unauthorised interference by personnel working in these areas, the Company has designed and applied procedures for working in secure areas, which apply to employees and external parties working in such areas and cover all activities taking place in those secure areas.

- **Clear desk and screen** – To reduce the risks of unauthorised access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours, a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities are adopted.

- **Equipment siting and protection** – Equipment and other assets, are sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access, including exposure to unintended audiences, which must be considered.

- **Security of assets off-premises** – To prevent loss, damage, theft or compromise of off-site devices and interruption to bluesource's operations, off-site assets must be suitably protected.

- **Storage Media** – To ensure only authorised disclosure, modification, removal, or destruction of information on storage media, the Company restricts the use of storage media and manages any authorised use through their lifecycle of acquisition, use, transportation, and disposal in accordance with the Company's data classification and handling requirements.

- **Supporting utilities** – To prevent loss, damage or compromise of information and other associated assets, or interruption to the Company's operations due to failure and disruption of supporting utilities, information processing facilities are protected from power failures and other disruptions caused by failures in supporting utilities as far as reasonably possible and commensurate with the level of risk to its operation. Cloud and SaaS are utilised to avoid supporting utilities affecting services and office-based systems connected to UPS technology.

- **Cabling Security** – To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the Company's operations related to power and communications cabling, power and telecommunications cabling carrying data or supporting information services is, as far as reasonably practical, protected from interception, interference, or damage wherever possible. Cloud and SaaS are utilised to further avoid such risk wherever possible.

- **Equipment maintenance** – Equipment is correctly maintained to ensure its continued availability and integrity. It is maintained in accordance with supplier recommendations by authorised personnel internally and the use of third-party maintenance agreements as applicable. Operational equipment and software are not out of vendor support.

- **Secure disposal or re-use of equipment** - All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. The Company has legal obligations to ensure that all computers, IT equipment, and data storage media (e.g., USB drives, DVDs, CDs, etc.) including the data and software held upon such equipment, are disposed of appropriately and legally.

Technical Security

Technology plays a big part in information security as well as providing tools to make it easier to apply controls that have already been discusses, and as part of its ISMS, the Company has put in place key technical security controls, which include:

- **User endpoint devices -** To protect information on a user endpoint device against risks introduced by using them, the Company has established a topic specific policy to protect such information stored on, processed by or accessible via such devices, against the risks introduced by using them. Access control, including multi-factor authentication, disk encryption, virus and malware protection, restricted local admin, technical controls play their part in helping to secure such devices.

- **Privileged access rights** - To ensure only authorised users, software components and services are provided with privileged access rights, the allocation and use of privileged access rights is restricted and managed by those authorised by the Company's senior management. Just-in-time access control is also in place to add further protection by allowing enhanced privileges for short periods of time, only as and when necessary.

- **Information access restrictions** - To ensure only authorised access and to prevent unauthorised access to information and other associated assets, access is restricted in accordance with the Company's topic specific policy on access control, with access controlled by the information owner on a need-to-know and minimum rights basis.

- **Access to source code** – Whilst bluesource does not generally build its own applications and uses third-party applications produced by reputable vendors, access to program source code and associated items (such as designs, specifications, verification plans and validation plans) is strictly controlled, to prevent the introduction of unauthorised functionality and to avoid unintentional changes, as well as to maintain the confidentiality of valuable intellectual property.

- **Secure Authentication** - To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted, secure authentication technologies and procedures have been implemented based on information access restrictions and its topic specific, "Access Control", policy.

- **Capacity Management** – To ensure the required performance of its systems, the Company monitors, tunes, and projects the use of its resources. Such activities ensure that the Company's systems have enough capacity to maintain its services.

- **Protection against malware** – To protect against malware, the Company has implemented malware detection, prevention and recovery controls and combine this with appropriate user awareness. A regular patching cycle is maintained for operating systems and applications. The Company applies the latest security patches and updates to operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities. Patch management processes are in place to implement security patch updates as they are released by vendors. Patches are tested prior to being deployed into production.

- **Management against technical vulnerabilities** - Information regarding technical vulnerabilities to the Company's information systems is obtained as soon as practicably possible and the Company's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. Information systems are regularly checked for compliance with the Company's information security polices and standards.

- **Configuration Management** - To ensure hardware, software, services, and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes, the Company establishes, documents, implements, monitors, and reviews the configurations, including security configurations, of hardware, software, services, and networks.

- **Information deletion** - To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory, and contractual requirements for information deletion, information stored in information systems, devices or any other storage media is deleted when no longer required. Retention policies are applied, wherever possible, with the Company's information is typically retained for 6+ years in line with its Data Processing Policy.

- **Data masking** - To limit the exposure of sensitive data including personally identifiable information ("PII"), password entry, and to comply with legal, statutory, regulatory, and contractual requirements, the Company considers data masking wherever possible and commensurate with the sensitivity of the data. The Company does not knowingly process "sensitive" data going by the DPA 2018 and GDPR definitions, and as such does not deem data masking necessary, other than to hash out passwords at point of entry and technical controls in place, to identify certain types of sensitive data, such as passport, bank details, NI number, etc., and automatically encrypt the document to restrict access.

- **Data leakage protection** - To detect and prevent the unauthorised disclosure and extraction of information by individuals or systems, the Company applies data leakage prevention measures to its systems, network and any other devices that process, store, or transmit sensitive information.

- **Information backup** - To enable recovery from loss of data or systems, the Company maintains and test backup copies of its information, software, and systems in accordance with its topic specific policy.

- **Redundancy of information processing facilities** - To ensure that continuous operation of information processing facilities, they are implemented with sufficient redundancy to meet the availability requirements of the Company, to satisfy that of any obligations, and commensurate with the service itself and business value. The Company's production systems are predominantly in the cloud wherever possible, utilising the high availability offered by such IAAS and SaaS solutions. With hybrid working in place, the Company does not currently require a secondary or DR location to be in place and details of recovery are maintained in the Company's DR and BCP plans.

- **Logging** - To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations, the Company produces, stores, protects and analyses logs that record activities, exceptions, faults, and other relevant events. This is automated wherever possible using technologies. Such logs provide an account of which personnel have accessed which systems and include security-relevant events. The event logs are protected from unauthorized access and tampering.

  Access to auditing and logging is further controlled by limiting access to authorized individuals. Potential security issues are triaged and escalated within security operations and to an incident response team accordingly. Security events that record critical system configuration changes or elevated permissions are alerted at the time of change. Retention schedules are defined with the Company's retention policy.

- **Monitoring activities -** To detect anomalous behaviour and potential information security incidents, the Company's networks, systems, and applications are monitored, where possible, for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

- **Clock synchronisation** - To enable the correlation and analysis of security related events and other recorded data, and to support investigations into information security incidents, the clocks of information processing systems used by the Company are synchronised to approved time sources.

- **Use of privileged utility programs** - To ensure the use of utility programs does not harm system and application controls for information security, utility programs that can be capable of overriding system and application controls are restricted and controlled.

- **Installation of software on operational systems** - To ensure the integrity of operational systems and prevent exploitation of any technical vulnerabilities, the Company has implemented procedures and measures to securely manage software installation on operational systems. Local admin restrictions and the utilisation of tools to assist with technical controls to aid such restrictions.

- **Network security** - To protect information in networks and its supporting information processing facilities from compromise via the network, networks and network devices are secured, managed, and controlled by the Company.

- **Security of network services** - To protect information in networks and its supporting information processing facilities from compromise via the network, networks and network devices are secured, managed, and controlled by the Company.

- **Segregation of networks** - to provide security boundaries and to control the traffic between them based on business needs, groups of information services, users and information systems are segregated in the Company's networks. The Company' maintains a separate guest wi-fi within its premise.

- **Web filtering** - To protect systems from being compromised by malware and to prevent access to unauthorised web resources, the Company manages access to external websites to reduce exposure to potential malicious and inappropriate content.

- **Use of cryptography** - To ensure proper and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory, and contractual requirements related to cryptography, the Company has defined and implemented rules and guidelines for the effective use of cryptography, including cryptographic key management.

- **Secure development lifecycle** - To ensure information security is designed and implemented within the secure development lifecycle of software and systems, whilst the Company does not develop its own software and systems, and uses that of established vendors and service providers, it has put together rules for the secure development of software and systems.

- **Application security requirements** - To ensure all information security requirements are identified and addressed when developing or acquiring applications, they are identified, specified, and approved by the Company, commensurate with the processing and level of risk, with a new information processing facility procedure is in place.

- **Secure system architecture and engineering principles** - To ensure information systems are securely designed, implemented, and operated within the development life cycle, principles for engineering secure systems should be established, documented, maintained, and applied to any information system development activities. At present the Company does not undertake any of its own development and uses applications and systems provided by market leading and reputable vendors. Best practice guidance is followed when establishing, seting up, using and maintaining applications and systems provided by such vendors.

- **Secure coding** - To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software, secure coding principles should be applied to any software development. As with system development detailed above, the Company does not do any software development or coding of its own and uses applications and systems provided by appropriate and reputable vendors.

Where technologies such as artificial intelligence or scripts are created to perform a task, care is taken to ensure they do what is intended and identify any potential risk with their use - These are not considered as writing software, in the same way as creating a database using a specific platform such as Filemaker, SQL and MS Access, etc.

- **Security testing in development and acceptance** - To validate if information security requirements are met when applications or code are deployed to the production environment, the Company defines and implements security testing processes in the development lifecycle. At present Company testing is limited to PEN testing and testing linked to change control as it does not conduct any inhouse software development.

  Should the Company start any in-house developments, tests should initially be performed by the development team and then followed up by independent acceptance testing to ensure that the system works as expected and only as expected.

- **Outsourced development** - To ensure information security measures required by the Company are implemented in outsourced system development, the Company uses commonly available software from reputable vendors to meet its needs, rather than utilising outsourced development of its own applications and systems.

- **Separation of development, test, and production environments** - To protect the production environment and data from compromise by development and test activities, the Company uses separate development, test, and production environments.

- **Change control** - To preserve information security when executing changes, changes to information processing facilities and information systems are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested, and monitored post-implementation to ensure that the expected changes are operating as intended.

- **Test information** - To ensure relevance of testing and protection of operational information used for testing, the Company appropriately selects, protects, and manages test information.

- **Protection of information systems during audit testing** - To minimise the impact of audit and other assurance activities on operational systems and business processes, any audit tests and other assurance activities involving assessment of operational systems are planned and agreed between the tester and appropriate management.