Control Group	Ref	Name	Control	Applicable (Yes/No)	Justification for any exclusion	Implementation Status	Comment	References	Owner	Date of Last Review	Additional Notes
Organisational Controls	5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes		Implemented	Policies documents created, starting with "Information Security Policy", and sub policies. These are all signed and approved by management and subject to a communication plan "	Information Security Policy Sub-policies Information Security Communications Plan			
Organisational Controls	5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organisation needs	Yes		Implemented	Roles & Responsibilities documented in each policy and procedure and in ISMS R&Rs documentation.	ISMS Roles & Responsibilities Document Information Security Steering Group Terms of Reference			
Organisational Controls	5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	Yes		Implemented	Access control is based upon the principle of least privilege and separation of permissions.	Access Control Policy			
Organisational Controls	5.4	Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation.	Yes		Implemented	A top down approach is taken to communication of responsibilities across the organisation to staff at all levels.	Information Security Statement Action plans from management meetings ISMS Objectives Information Security Communications Plan			
Organisational Controls	5.5	Contact with authorities	The organisation should establish and maintain contact with relevant authorities.	Yes		Implemented	In the UK, the key point of contact is the ICO for personal data breaches under GDPR, PECR, NIS and other directives. The contact details and procedure is outlined in the incident response plan and Data Protection policy. Incident management records will document any external contact with agencies or customers.	Cyber Security Incident Response Plan Data Protection Policy Incident Management Records			
Organisational Controls	5.6	Contact with special interest groups	The organisation should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes		Implemented	Staff have registered with specialist forums and are regularly updated as to new practices and emerging threats. A list is maintained of the groups and memberships.	Special Interest Groups & Forums document			
Organisational Controls	5.7	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	Yes		Implemented	Membership of forums, newsletters and external groups provides up to date knowledge and warning of emerging threats.	Special Interest Groups & Forums document			
Organisational Controls	5.8	Information security in project management	Information security should be integrated into project management.	Yes		Implemented	Guidance is provided to all projects regardless of their size to ensure security is baked into the solution from the outset. A development policy and guidelines are also available.	M2 Secure Development Guidelines, P10 Secure Development Policy, M3 Project Management Guidelines			
Organisational Controls	5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Yes		Implemented	All assets are maintained in an inventory, including laptops and other hardware, and information assets.	P12 Asset Management Policy, R1 Asset Inventory			
Organisational Controls	5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Yes		Implemented	An acceptable use policy is in place	P2 Acceptable use policy			
Organisational Controls	5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.	Yes		Implemented	The return of company assets is outlined in several policies outlining the responsibilities for the return of all company assets upon termination of employment or contracts and specifying procedures to prevent unauthorised retention or reuse of organisational information and assets.	P2 Acceptable use policy, P1 Information Security Policy, P12 Asset Management Policy, R1 Asset Inventory			
Organisational Controls	5.12	Classification of information	Information should be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements.	Yes		Implemented	The Information Security Policy (P1) addresses control 5.12 by defining a clear classification scheme for information, documenting and communicating it to relevant personnel, and providing specific handling guidelines for each classification level to ensure proper protection based on sensitivity and criticality.	P1 Information Security Policy			
Organisational Controls	5.13	Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Yes		Implemented	The Information Security Policy (P1), supported by the Asset Management Policy (P12) and Asset Inventory (R1), meets the requirements of control 5.13 by providing a clear classification scheme, detailing handling guidelines, and emphasizing training and awareness.	P1 Information Security Policy, P12 Asset Management Policy, R1 Asset Inventory			

Organisational Controls	5.14	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organisation and between the organisation and other parties.	Yes	Implemented	The Information Security Policy (P1) meets the requirements of control 5.14 by establishing comprehensive rules and procedures for the secure transfer of information, both electronically and physically. It ensures information is protected in transit, maintains traceability, and includes necessary transfer agreements and labelling systems.	P1 Information Security Policy
Organisational Controls	5.15	Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Yes	Implemented	The policies collectively meet the requirements of control 5.15 by ensuring relevant information security requirements are included in third-party agreements, defining supplier obligations, including incident management procedures, ensuring confidentiality agreements, and emphasizing periodic review of these agreements.	P1 Information Security Policy, P3 Access Control Policy
Organisational Controls	5.16	Identity management	The full life cycle of identities should be managed.	Yes	Implemented	The Access Control Policy (P3) and Information Security Policy (P1) collectively meet the requirements of control 5.16 by ensuring unique identification, managing the identity lifecycle, documenting shared identities, managing non-human entities, timely disabling/removing identities, maintaining event records, verifying identities, and ensuring third-party identities meet trust requirements.	P1 Information Security Policy, P3 Access Control Policy
Organisational Controls	5.17	Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Yes	Implemented	The policies meet the requirements of control 5.17 by establishing comprehensive policies and procedures for managing user access and secret authentication information. This includes detailed guidelines on password creation, the use of multi-factor authentication, regular reviews of access rights, and procedures for reporting compromised passwords.	P8 Password policy, P3 Access Control Policy, P1 Information Security Policy
Organisational Controls	5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.	Yes	Implemented	Comprehensive policies and procedures for system and application access control exist. This includes proper authorization, documentation, regular reviews, segregation of duties, and robust access control mechanisms for protecting sensitive information.	P8 Password policy, P3 Access Control Policy, P1 Information Security Policy, P2 Acceptable Use Policy
Organisational Controls	5.19	Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	Implemented	The Supplier Security Policy and Supplier Performance Reviews, supported by the Access Control Policy and Information Security Policy, collectively meets the requirements of ISO 27002:2022 control 5.19 by defining and implementing comprehensive processes and procedures to manage information security risks in supplier relationships. This includes thorough risk identification and assessment, detailed contractual security requirements, regular monitoring and review of supplier performance and compliance, and effective incident management.	P11 Supplier Security Policy, P3 Access Control Policy, P1 Information Security Policy, R5 Supplier Performance Review records
Organisational Controls	5.20	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Yes	Implemented	The Supplier Security Policy meets the requirements of ISO 27002:2022 control 5.20 by establishing and documenting comprehensive information security requirements within supplier agreements. It ensures a clear understanding of obligations between the organisation and suppliers, covering confidentiality, asset return, compliance with security standards, and regular monitoring and review.	P11 Supplier Security Policy

Organisational Controls	5.21	Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	Implemented	The Supplier Security Policy meets the requirements of ISO 27002:2022 control 5.21 by defining and implementing comprehensive processes and procedures to manage information security risks in the ICT supply chain. It ensures that security requirements are propagated through the supply chain, includes robust monitoring and evaluation methods, addresses critical component assurance, and provides effective incident management.	P11 Supplier Security Policy
Organisational Controls	5.22	Monitoring, review and change management of supplier services	The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	Implemented	The Supplier Security Policy and Supplier Performance Review Template collectively meet the requirements of ISO 27002:2022 control 5.22 by implementing comprehensive risk management processes, including specific information security requirements in supplier agreements, regularly monitoring and reviewing supplier performance, managing security incidents effectively, and ensuring proper procedures for the termination of supplier relationships.	P11 Supplier Security Policy, R5 Supplier Performance Review
Organisational Controls	5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.	Yes	Implemented	The Cloud Service Catalogue (R6), SaaS & Cloud Services Policy (P13), and Supplier Security Policy (P11) collectively address the requirements of control 5.23. They provide comprehensive guidelines for managing cloud services, conducting risk assessments, enforcing security requirements, implementing access controls, ensuring data protection, and monitoring and reviewing cloud service performance.	R6 Cloud Service Catalogue, P13 Cloud Services Policy, P11 Supplier Security Policy
Organisational Controls	5.24	Information security incident management planning and preparation	The organisation should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities	Yes	Implemented	The Major Incident Report Template (IR 2), Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), and Supplier Security Policy (P11) collectively address the requirements of ISO 27002:2022 control 5.24. They establish comprehensive procedures for managing information security incidents in the ICT supply chain, ensure suppliers comply with notification requirements, and emphasize the importance of post-incident reviews to improve future incident management and supplier relationships.	IR2 Major Incident Reports, IR3 Cyber Security Incident Response Plan, IR1, Incident & Major Incident Processes, P11 Supplier Security Policy
Organisational Controls	5.25	Assessment and decision on information security events	The organisation should assess information security events and decide if they are to be categorised as information security incidents.	Yes	Implemented	The Cyber Security Incident Response Plan (IR 3) and Incident & Major Incident Processes (IR 1) address the requirements of ISO 27002:2022 control 5.25 by providing comprehensive procedures for assessing information security events, categorizing and prioritizing them, and maintaining detailed documentation of assessments and decisions.	IR3 Cyber Security Incident Response Plan, IR 1 Incident & Major Incident Processes
Organisational Controls	5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Yes	Implemented	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), and Supplier Security Policy (P11) collectively address the requirements of ISO 27002:2022 control 5.26 by establishing comprehensive and documented procedures for responding to information security incidents. They ensure designated teams handle incidents, include necessary response steps, integrate with crisis management, and maintain detailed logs of incident management activities.	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), Supplier Security Policy (P11)

Organisational Controls	5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Yes	Implemented	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), and Supplier Security Policy (P11) collectively address the requirements of ISO 27002:2022 control 5.27 by establishing procedures to quantify and monitor information security incidents, conducting post-incident analyses, updating the incident management plan, and using insights to enhance user awareness and training.	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), Supplier Security Policy (P11)
Organisational Controls	5.28	Collection of evidence	The organisation should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	Implemented	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), Major Incident Report Template (IR 2), and Supplier Security Policy (P11) collectively address the requirements of ISO 27002:2022 control 5.28 by establishing procedures for the identification, collection, acquisition, and preservation of evidence related to information security events. They also ensure the proper documentation of evidence handling to support disciplinary and legal actions, maintaining the integrity and admissibility of the evidence.	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), Major Incident Report Template (IR 2), Supplier Security Policy (P11)
Organisational Controls	5.29	Information security during disruption	The organisation should plan how to maintain information security at an appropriate level during disruption.	Yes	Implemented	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), and Supplier Security Policy (P11) collectively address the requirements of ISO 27002:2022 control 5.29 by developing and implementing information security continuity plans, ensuring regular testing and updates, coordinating with business continuity plans, and maintaining thorough documentation.	The Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1), Supplier Security Policy (P11)
Organisational Controls	5.30	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	Implemented	The Disaster Recovery Plan (G12), Cyber Security Incident Response Plan (IR 3), and Incident & Major Incident Processes (IR 1) collectively address the requirements of ISO 27002:2022 control 5.30 by establishing ICT continuity plans, ensuring regular testing and updates, coordinating with business continuity plans, and maintaining thorough documentation and communication.	The Disaster Recovery Plan (G12), Cyber Security Incident Response Plan (IR 3), Incident & Major Incident Processes (IR 1)
Organisational Controls	5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements should be identified, documented and kept up to date.	Yes	Implemented	The Statutory Regulatory & Contractual Requirements document (G11), Disaster Recovery Plan (G12), and Cyber Security Incident Response Plan (IR 3) collectively address the requirements of ISO 27002:2022 control 5.31 by identifying and documenting applicable requirements, specifying regular review processes, ensuring communication to relevant stakeholders, and ongoing compliance monitoring.	Statutory Regulatory & Contractual Requirements document (G11), Disaster Recovery Plan (G12), Cyber Security Incident Response Plan (IR 3)
Organisational Controls	5.32	Intellectual property rights	The organisation should implement appropriate procedures to protect intellectual property rights.	Yes	Implemented	The Statutory Regulatory & Contractual Requirements document (G11), Information Security Policy (P1), and SaaS & Cloud Services Policy (P13) collectively address the requirements of ISO 27002:2022 control 5.32 by identifying and documenting IP rights, implementing measures to protect these rights, ensuring compliance with IP laws, and promoting awareness and training on IP rights.	Statutory Regulatory & Contractual Requirements document (G11), Information Security Policy (P1), SaaS & Cloud Services Policy (P13)
Organisational Controls	5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorised access and unauthorised release.	Yes	Implemented	It is likely your system (google, SharePoint, 365, etc) manages this for you, allowing for historical views of documents and who updated what, when.	
Organisational Controls	5.34	Privacy and protection of PII	The organisation should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Implemented	The Information Security Policy, Data Protection Policy, and Data Retention Policy collectively ensure compliance with ISO 27002:2022 control 5.34, establishing and implementing procedures for the preservation of privacy and protection of PII.	The Information Security Policy, Data Protection Policy, Data Retention Policy

Organisational Controls	5.35	Independent review of information security	The organisation's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Yes	Implemented	External Audit Reports, Certifications & Assessments from Pen Test Results, etc.	External Audit Reports, Certifications & Assessments, Pen Test Results
Organisational Controls	5.36	Compliance with policies, rules and standards for information security	Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Yes	Implemented	The Information Security Policy includes procedures for regular reviews and audits, ensuring compliance with the organisation's information security policies, rules, and standards. All policies must be reviewed at least annually.	
Organisational Controls	5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Yes	Implemented	See M4 Standard Operating Procedures	M4 Standard Operating Procedures
People Controls	6.1	Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Implemented	The Information Security Policy includes procedures for conducting background checks as part of the employment process, ensuring compliance with ISO 27002:2022 control 6.1. Additionally, the Risk Treatment Plan for Insider Threats outlines the practice of background checks to mitigate potential risks associated with new hires.	Information Security Policy, ISO 27002:2022, Risk Treatment Plan for Insider Threats
People Controls	6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organisation's responsibilities for information security.	Yes	Implemented	[Insert evidence of staff contracts]	
People Controls	6.3	Information security awareness, education and training	Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.	Yes	Implemented	The Information Security Communications Plan includes a comprehensive awareness campaign, covering essential information security topics. This plan ensures all employees receive ongoing education and training, aligning with ISO 27002:2022 control 6.3. Newly inducted staff are sign-posted to all materials and policies. R4 - Training Competency records are maintained for all staff who are required to take specific / advanced information security training for their roles.	Information Security Communications Plan, R4 - Training Competency records
People Controls	6.4	Disciplinary process	A disciplinary process should be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	Implemented	The organisation has a disciplinary process, and policies underline the need for compliance.	
People Controls	6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Yes	Implemented	Our policies, including the Information Security Policy, Access Control Policy, Acceptable Use Policy, and BYOD Policy, collectively address responsibilities after termination or change of employment. These policies ensure access rights are revoked, company assets are returned, and data is securely handled. [Include reference to any leavers procedure]	Information Security Policy, Access Control Policy, Acceptable Use Policy, BYOD Policy
People Controls	6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Implemented	[Insert evidence of any non-disclosure legal agreements or clauses in contracts].	
People Controls	6.7	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	Yes	Implemented	The Remote Working Policy, Acceptable Use Policy, and Information Security Policy collectively ensure compliance by providing comprehensive guidelines and procedures for secure remote working, covering aspects such as secure remote access, device security, data handling, incident reporting, physical security, and compliance monitoring.	Remote Working Policy, Acceptable Use Policy, Information Security Policy
People Controls	6.8	Information security event reporting	The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	Implemented	The Information Security Policy, Acceptable Use Policy, and Remote Working Policy collectively support ISO 27002:2022 control 6.8 by ensuring system activity monitoring, logging, and compliance with relevant laws. To fully align with the control, enhance these policies with detailed logging procedures, baseline and anomaly detection methods, and the use of advanced monitoring tools which are unique to your organisation's infrastructure.	The Information Security Policy, Acceptable Use Policy, Remote Working Policy

Physical Controls	7.1	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Yes	Implemented	The organisation has implemented access control systems for secure areas, including card readers and biometric scanners, managed by the Facilities Manager and Security Personnel. Access requests are processed through a formal approval system. The Access Control to Physical Locations SOP establishes guidelines for setting up, monitoring, and maintaining physical security perimeters to protect information processing facilities, ensuring only authorised personnel have access.	Access Control to Physical Locations SOP
Physical Controls	7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Yes	Implemented	Physical entry to secure areas is controlled through a formal access request and approval process, issuance of access credentials, and continuous monitoring using security cameras and access logs. The Access Control to Physical Locations SOP includes measures for installing and configuring access control systems (e.g., card readers, biometric scanners), maintaining logs of access events, and regularly reviewing access permissions to secure physical entry points.	Access Control to Physical Locations SOP, access logs
Physical Controls	7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Yes	Implemented	Security measures, including access control systems and continuous monitoring, are applied to offices, rooms, and facilities to ensure the protection of sensitive information and assets. The Access Control to Physical Locations SOP outlines procedures for securing offices, rooms, and facilities, including continuous monitoring and review of access controls to prevent unauthorised access.	Access Control to Physical Locations SOP
Physical Controls	7.4	Physical security monitoring	Premises should be continuously monitored for unauthorised physical access.	Yes	Implemented	Real-time monitoring and detailed logging of access events are conducted to ensure security in secure areas, with periodic reviews to address anomalies or unauthorised access. The Access Control to Physical Locations SOP ensures real-time monitoring of physical access using security cameras and access control logs, with established procedures for periodic reviews and incident response	Access Control to Physical Locations SOP, access control logs
Physical Controls	7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Yes	Implemented	Physical security measures, including the use of key or swipe cards, are in place to protect against physical threats. Environmental controls are implemented to mitigate risks. The Information Security Policy includes guidelines for protecting information processing facilities against physical and environmental threats, ensuring the resilience and security of critical assets.	Information Security Policy
Physical Controls	7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented.	Yes	Implemented	Procedures for working in secure areas include controlled access authorization and continuous monitoring to ensure security compliance. "Access Control to Physical Locations SOP" outlines the procedures for access authorization and monitoring (Sections 4 and 5)	Access Control to Physical Locations SOP
Physical Controls	7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Yes	Implemented	The "Acceptable Use Policy" includes clear desk and screen policies (Section on Clear Desk & Screen).	Acceptable Use Policy, Section on Clear Desk & Screen
Physical Controls	7.8	Equipment siting and protection	Equipment should be sited securely and protected.	Yes	Implemented	The "Information Security Policy" covers securing equipment through physical restrictions (Section on Physical Security). The Remote Working Policy includes guidelines for the secure siting and protection of equipment used remotely, reducing risks from environmental threats and unauthorised access.	Information Security Policy, Remote Working Policy

Physical Controls	7.9	Security of assets off-premises	Off-site assets should be protected.	Yes	Implemented	The "Acceptable Use Policy" and "Information Security Policy" both address remote working and the protection of mobile devices (Sections on Remote Working and Mobile Storage Devices).	Acceptable Use Policy, Information Security Policy
Physical Controls	7,10	Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.	Yes	Implemented	The Acceptable Use Policy mandates the secure management of storage media, including the use of encryption and secure handling procedures to protect sensitive data.	
Physical Controls	7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Implemented	The Information Security Policy ensures that supporting utilities are secured and properly maintained, supporting the continuous operation and security of information processing facilities.	
Physical Controls	7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Yes	Implemented	The Access Control to Physical Locations SOP includes measures to secure physical infrastructure, implicitly covering the protection of power and telecommunications cabling from interception or damage.	Access Control to Physical Locations SOP
Physical Controls	7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	Implemented	The Information Security Policy includes guidelines for the regular maintenance of information processing equipment to ensure its availability and integrity.	
Physical Controls	7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Implemented	The "Acceptable Use Policy" and "Information Security Policy" cover the secure disposal of equipment and data (Sections on Actions upon Leaving and Handling Guidance for Confidential Information).	Acceptable Use Policy, Information Security Policy
Technological Controls	8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Yes	Implemented	The BYOD and Mobile Device Policies outline comprehensive security measures for user endpoint devices, including strong authentication, encryption, antivirus software, and incident reporting procedures to protect against unauthorised access and threats.	BYOD and Mobile Device Policies
Technological Controls	8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	Yes	Implemented	The Access Control Policy includes strict guidelines for managing privileged access rights, ensuring that only authorised users have the necessary privileges and that these rights are regularly reviewed and audited.	Access Control Policy
Technological Controls	8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Yes	Implemented	The Access Control Policy and Information Security Policy enforce the principle of least privilege by ensuring that access rights are granted based on roles and responsibilities, regularly reviewed, and updated as needed.	Access Control Policy, Information Security Policy
Technological Controls	8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	Yes	Implemented	The Information Security Policy enforces access controls to sensitive information, including source code, ensuring that only authorised personnel can access and modify it."	
Technological Controls	8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	Implemented	The Access Control and Mobile Device Policies enforce strict password management practices, including the use of strong passwords, regular updates, and secure storage, to protect secret authentication information.	Access Control and Mobile Device Policies
Technological Controls	8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Yes	Implemented	The Access Control and Mobile Device Policies enforce strict password management practices, including the use of strong passwords, regular updates, and secure storage, to protect secret authentication information.	Access Control and Mobile Device Policies
Technological Controls	8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	Yes	Implemented	The Acceptable Use Policy and Mobile Device Policy mandate the use of antivirus software, anti-ransomware tools, and web filtering to protect against malware.	Acceptable Use Policy, Mobile Device Policy
Technological Controls	8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Yes	Implemented	The Information Security Policy includes processes for identifying, assessing, and mitigating technical vulnerabilities, ensuring that systems are regularly updated to address new security threats. A Patching Policy and Vulnerability Management SOP also exist to provide guidance.	

Technological Controls	8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Yes	Implemented	The Access Control Policy outlines procedures for the secure configuration and management of information systems, ensuring their integrity and security
Technological Controls	8.10	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Yes	Implemented	The Access Control Policy outlines procedures for the secure configuration and management of information systems, ensuring their integrity and security
Technological Controls	8.11	Data masking	Data masking should be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	Implemented	Our Secure Development Policy includes specific data masking techniques such as substitution, shuffling, redaction, and encryption. These techniques are integrated into the secure development lifecycle, ensuring that sensitive data, including PII, is protected during processing, storage, and transmission. Regular audits and security assessments ensure the effectiveness of our data masking practices.
Technological Controls	8.12	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	Implemented	Our organisation has implemented comprehensive data leakage prevention measures, including the deployment of DLP tools, monitoring and controlling data channels, restricting unauthorised data transfers, and providing regular employee training.
Technological Controls	8.13	Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	Implemented	Our organisation has implemented a comprehensive backup policy that includes regular backups of information, software, and systems. These backups are encrypted and stored securely. We conduct regular tests to ensure that backups can be successfully restored, and we continuously monitor and update our backup procedures to maintain data availability and integrity. The Data Protection Policy, Data Retention Policy, and Cloud Services Policy collectively support Control 8.13 by addressing backup frequency, secure storage, regular testing, and procedures for handling backups in both local and cloud environments.
Technological Controls	8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Yes	Implemented	Our organisation has implemented comprehensive redundancy measures for critical information processing facilities. These measures include geographic redundancy, high availability solutions, and regular backups and replication. Our Disaster Recovery Plan outlines detailed steps for maintaining redundancy and ensuring continuous operation and availability in case of a failure. Regular testing and maintenance ensure the effectiveness of our redundancy systems. The Disaster Recovery Plan, along with the Data Protection Policy, Data Retention Policy, and Cloud Services Policy, collectively support Control 8.14
Technological Controls	8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Yes	Implemented	The combined implementation of the Network Monitoring & Logging SOP, Information Security Policy, and Metrics & Reporting Approach ensures compliance with Control 8.15. These documents provide comprehensive guidelines for continuous monitoring, log capture, analysis, retention, and protection, as well as regular reporting and review of key metrics derived from logs to support security investigations and incident response

Technological Controls	8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	Implemented	The requirements for Control 8.16 (Monitoring Activities) are met through the combined implementation of the Network Monitoring & Logging SOP, Information Security Policy, and Metrics & Reporting Approach. These documents provide guidelines for continuous monitoring of network traffic, anomaly detection, real-time alerts, and regular analysis and reporting of key metrics. They ensure that networks, systems, and applications are monitored for anomalous behaviour, and appropriate actions are taken to evaluate and respond to potential information security incidents.
Technological Controls	8.17	Clock synchronization	The clocks of information processing systems used by the organisation should be synchronized to approved time sources.	Yes	Implemented	The requirements for Control 8.17 (Clock Synchronization) are addressed by the updated Network Monitoring & Logging SOP. This document specifies that all network devices, servers, and security appliances must synchronize their clocks with an approved time source using the Network Time Protocol (NTP). The IT Administrator is responsible for configuring and monitoring clock synchronization, with regular audits conducted to verify accuracy and synchronization of system clocks. This ensures accurate time-stamping for security-related events and supports effective forensic investigations
Technological Controls	8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Yes	Implemented	The requirements for Control 8.18 (Use of Privileged Utility Programs) are addressed by updating the Network Monitoring & Logging SOP to include procedures for managing, authorizing, and logging the use of utility programs that can override system and application controls. This ensures that only trusted, authorised users have access to these programs, and all usage is logged for audit purposes
Technological Controls	8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Yes	Implemented	The Acceptable Use Policy stipulates that only authorised IT personnel can install software on operational systems, following a defined process that includes authorization, verification, testing, and logging to ensure the integrity and security of operational systems.
Technological Controls	8.20	Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Yes	Implemented	The requirements for Control 8.20 (Network Security) are addressed through the Network Monitoring & Logging SOP, Acceptable Use Policy, and Asset Management Policy. These documents provide guidelines for continuous monitoring, logging, and protection of network activity, appropriate use of network devices, malware protection, and secure management of network assets.
Technological Controls	8.21	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Yes	Implemented	The requirements for Control 8.21 (Security of Network Services) are addressed through the Network Monitoring & Logging SOP. This document outlines the deployment and configuration of network monitoring tools to capture and analyse network traffic, supporting the secure management of network services. It includes procedures for continuous monitoring, real-time alerting, and incident management, ensuring that network services are securely managed and monitored

Technological Controls	8.22	Segregation of networks	Groups of information services, users and information systems should be segregated in the organisation's networks.	Yes	Implemented	The requirements for Control 8.22 (Segregation of Networks) are partially addressed by the Network Monitoring & Logging SOP. This document specifies the scope of network monitoring, including the definition of monitored devices, systems, and traffic types, which supports network segregation. It emphasizes the need for baseline performance metrics and continuous traffic analysis to maintain effective segregation and monitoring of network segments
Technological Controls	8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Yes	Implemented	Summarise any web filtering tools in place.
Technological Controls	8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Yes	Implemented	The Information Security Policy and Secure Development Policy comprehensively address Control 8.24 by outlining detailed procedures for cryptographic key management, specifying the use of approved cryptographic algorithms, and ensuring compliance with relevant regulations. These policies collectively ensure that cryptographic measures are effectively implemented and managed to protect sensitive information.
Technological Controls	8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	Yes	Implemented	The Secure Development Policy establishes comprehensive rules for the secure development of software and systems, including secure coding practices, environment separation, and security checkpoints throughout the development lifecycle, ensuring information security is integrated and maintained .
Technological Controls	8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Yes	Implemented	The Secure Development Policy requires that all security requirements be identified, specified, and approved during the development and acquisition of applications, incorporating necessary security measures such as data protection, access control, and secure communication .
Technological Controls	8.27	Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Yes	Implemented	The Secure Development Policy incorporates principles for secure system architecture and engineering, ensuring security is designed into all layers of the architecture and maintaining compliance with security standards and practices .
Technological Controls	8.28	Secure coding	Secure coding principles should be applied to software development.	Yes	Implemented	The Secure Development Policy mandates the application of secure coding principles, including regular code reviews, static and dynamic analysis, and adherence to secure coding standards to minimize vulnerabilities and ensure robust software security .
Technological Controls	8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	Yes	Implemented	The Secure Development Policy includes procedures for continuous security testing throughout the development lifecycle, encompassing static and dynamic analysis, penetration testing, and vulnerability scanning to identify and address security issues promptly .
Technological Controls	8.30	Outsourced development	The organisation should direct, monitor and review the activities related to outsourced system development.	Yes	Implemented	The Supplier Security Policy ensures that outsourced development activities comply with the organisation's security requirements, including secure design, coding, and testing practices, and mandates ongoing monitoring and review of supplier compliance.
Technological Controls	8.31	Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	Yes	Implemented	The Secure Development Policy requires the separation and security of development, test, and production environments, preventing unauthorised access and ensuring that production environments are protected from development and test activities .

Technological Controls	8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Yes	Implemented	The Change Management SOPs, including Change Request and Approval, Change Implementation & Testing, and Change Documentation & Review, collectively ensure thorough technical reviews of applications after operating platform changes. These procedures include comprehensive impact assessments, detailed documentation, and rigorous post implementation testing, aligning with Control 8.32 requirements
Technological Controls	8.33	Test information	Test information should be appropriately selected, protected and managed.	Yes	Implemented	The Secure Development Policy mandates the use of data masking techniques and secure handling of sensitive data in test environments, ensuring that test information is protected and managed appropriately. These measures include the substitution, shuffling, redaction, and encryption of sensitive data, providing comprehensive protection during testing .
Technological Controls	8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Yes	Implemented	The Information Security Policy requires that all access requests and scope of technical audits be agreed upon and controlled by appropriate management, limiting audit tests to read-only access where possible. This ensures minimal impact on operational systems and maintains confidentiality, integrity, and availability during audit and assurance activities .