In order to ensure that eSentire is able to meet regulatory, industry and customer obligations, eSentire has implemented an Information Security Management System based on the ISO/IEC 27001:2013 standard. The purpose of this document is to define which controls are appropriate for eSentire, Inc., the objectives of the controls, and describe at a high level how they are implemented. This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information systems Management Scope.

Control	Control Objective	Applicability	Rationale for Inclusion/Exclusion	Implementation	Stakeholders
		Waterloo, ON			
A.5.1.1	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Security policies have been established and communicated that define the information security requirements.	CISO, CTO, CIO, Legal, IT, and Development.
A.5.1.2	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Security policies are reviewed, approved, and updated as needed (at least annually).	CISO, CTO, CIO, Legal, IT, and Development.
A.6.1.1	All information security responsibilities shall be defined and allocated.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	CISO, CTO, Chief Privacy Officer, etc. each have accountability for assigned aspects of the enterprise-wide information security program.	CISO, CTO, CIO, Legal, IT, and Development.
A.6.1.2	All information security responsibilities shall be defined and allocated.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Roles and responsibilities for production systems have been distributed so adequate segregation of duties exists (e.g., developers do not have unattended or untraceable access to production, etc.).	CISO, CTO, CIO, Legal, IT, and Development.
A.6.1.3	Appropriate contacts with relevant authorities shall be maintained.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Legal, Privacy, and IR team maintain the policy and procedures for engaging authorities when a data breach or other information security incident triggers a notification obligation.	CISO, CTO, CIO, Legal, IT, and Development.
A.6.1.4	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Individuals from Legal, Privacy, Threat Intelligence, etc. are active participants in industry groups.	CISO, CTO, CIO, Legal, IT, and Development.
A.6.1.5	Information security shall be addressed in project management, regardless of the type of the project.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The CISO office, including Privacy, is engaged in product design and evaluating security controls.	CISO, CTO, CIO, Legal, IT, and Development.
A.6.2.1	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Antivirus software is installed on corporate issued laptops and Windows production servers and is configured to automatically update signature definitions. Acceptable use policy outlines use requirements for corporate assets.	CISO, CTO, CIO, Legal, IT, and Development.
A.6.2.2	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Access to corporate systems/resources requires two factor authentication and/or use of VPN.	CISO, CTO, CIO, Legal, IT, and Development.
A.7.1.1	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	New hires undergo screening and background checks, where legally permitted, during the hiring process.	CISO, CTO, CIO, Legal, IT, and Development.
A.7.1.2	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Employment agreements include confidentiality obligations and the Employee Handbook outlines additions security obligations.	CISO, CTO, CIO, Legal, IT, and Development.
A.7.2.1	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Employees are required to attest to their understanding and acceptance of their information security obligations on an annual basis.	CISO, CTO, CIO, Legal, IT, and Development.
A.7.2.2	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	New employees undergo Information Security education and awareness during their orientation. Additional security training is regularly provided.	CISO, CTO, CIO, Legal, IT, and Development.

A.7.2.3	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Employees who violate corporate policy and/or the terms of their employment agreement may be subject to disciplinary action up to and including termination.	CISO, CTO, CIO, Legal, IT, and Development.
A.7.3.1	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Relevant clauses in the NDA and employment agreement survive the termination of employment.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.1.1	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The following asset information is maintaind for all physical assets: - asset label; - type/category of asset; and - asset location.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.1.2	Assets maintained in the inventory shall be owned.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All assets are owned by the company and included in the asset inventory.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.1.3	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Acceptable Use Policy, Privacy Policy, and other corporate security policies describe the acceptable use of company assets and information, appropriate data handling standards, and management of physical assets.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.1.4	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Upon termination, employees, contractors, and vendors must return all corporate assets assigned to them.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.2.1	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Information is classified in accordance with its confidentiality and sensitivity.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.2.2	An appropriate set of procedures for information labelling shall bedeveloped and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Information is labeled and handled according to the Information Security Requirements.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.2.3	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Information Security Policy specifies the handling procedures of classified data elements.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.3.1	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Removable media is prohibited for use on critical assets and information except where authorized by management.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.3.2	Media shall be disposed of securely when no longer required, using formal procedures.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Decommissioned devices are securely wiped and/or physically destroyed. Re-used equipment must be securely wiped prior to being repurposed.	CISO, CTO, CIO, Legal, IT, and Development.
A.8.3.3	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Physical media is transported based on the Information Security Policy. Requests to transport media are documented and approved within the internal ticketing system.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.1.1	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Information Security Policy describes the logical access controls in place to limit access to confidential information.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.1.2	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Systmes access is provided based on the principal of least privilege as specified in the Information Security Policy.	CISO, CTO, CIO, Legal, IT, and Development.

A.9.2.1	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	New or modified access to the corporate network is authorized based on job function and/or business need. Access to the corporate network is revoked in a timely manner.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.2.2	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	New or modified access to the corporate network is authorized based on job function or a business need. Access to the corporate network is revoked in a timely manner.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.2.3	The allocation and use of privileged access rights shall be restricted and controlled.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	New or modified access to the corporate network is authorized restricted to only those who require access to perform their role.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.2.4	The allocation of secret authentication information shall be controlled through a formal management process.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Password standards and policies regarding the use and protection of passwords have been established and implemented.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.2.5	Asset owners shall review users' access rights at regular intervals.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Production access is reviewed quarterly to validate the appropriateness of user accounts. Users no longer requiring access are removed.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.2.6	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Production access is revoked in a timely manner upon termination.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.3.1	Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Password standards and policies regarding the use and protection of passwords have been established and implemented.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.4.1	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	New or modified access to the corporate or production networks is authorized based on job function or a business need.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.4.2	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All corporate laptops are configured with an idle timeout of 10 minutes.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.4.3	Password management systems shall be interactive and shall ensure quality passwords.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Passwords are managed, where applicable, through Active Directory.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.4.4	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Use of system utilities is restricted.	CISO, CTO, CIO, Legal, IT, and Development.
A.9.4.5	Access to program source code shall be restricted.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Source code is restricted to authorized users.	CISO, CTO, CIO, Legal, IT, and Development.
A.10.1.1	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Information Security Requirements describes the management of the encryption key process.	CISO, CTO, CIO, Legal, IT, and Development.
A.10.1.2	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Information Security Requirements describes the management of the encryption key process.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.1.1	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Physical access to the SOC is restricted through the use of two factor authentication.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.1.2	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All buildings are equipped with CCTV, badge readers, and manned reception areas.	CISO, CTO, CIO, Legal, IT, and Development.

A.11.1.3	Physical security for offices, rooms and facilities shall be designed and applied.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All buildings are equipped with CCTV, badge readers, and manned reception areas.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.1.4	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Access restrictions, disaster recovery plans, system failover, and geographic separation of facilities are in place to minimize potential damage from physical and environmental hazards and malicious threats.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.1.5	Procedures for working in secure areas shall be designed and applied.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	SOC access requires approval based on job function.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.1.6	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Access to eSentire premises is protected via physcial access controls and receptionists and/or security guards.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.1	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Access restrictions, disaster recovery plans, system failover, and geographic separation of facilities are in place to minimize potential damage from physical and environmental hazards and malicious threats.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.2	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All facilities have adequate uninterruptable power supply (UPS) and backup generator units to provide back-up power in the event of an electrical failure and to facilitate an orderly shutdown. HVAC systems are in place to maintain appropriate atmospheric conditions.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.3	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Fire detection and suppression equipment is in place in office facilities and data centers that meet legal and regulatory requirements.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.4	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Patching is performed, as needed, to remediate critical or high risk vulnerabilities identified through penetration testing or vulnerability scans. Preventative equipment maintenance is performed per preventative maintenance schedules.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.5	Equipment, information or software shall not be taken off-site without prior authorization.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Decommissioned devices are securely wiped and/or physically destroyed. Re-used equipment must be securely wiped prior to being repurpose.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.6	Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Acceptable Use Policy and the Information Security Policy detail the relevant information security practices.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.7	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Decommissioned devices are securely wiped and/or physically destroyed. Re-used equipment must be securely wiped prior to being repurposed.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.8	Users shall ensure that unattended equipment has appropriate protection.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Corporate laptops are configured with an idle timeout of 10 minutes.	CISO, CTO, CIO, Legal, IT, and Development.
A.11.2.9	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Information Security Policy describes the relevant practices.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.1.1	Operating procedures shall be documented and made available to all users who need them.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Internal teams use Sharepoint, Jira, and Confluence for their documented processes and procedures.	CISO, CTO, CIO, Legal, IT, and Development.

A.12.1.2	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Change management is approved and documented in an internal ticketing system and relevant changes are tested prior to being deployed to production.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.1.3	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Capacity planning is performed regularly by IT to evaluate current system needs and meet availability commitments.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.1.4	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Access to the development and testing environments is restricted and maintained separately from the list of users with access to the production environment.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.2.1	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Antivirus software is installed on corporate issued laptops and Windows production servers and is configured to automatically updated signature definitions.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.3.1	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	IT regularly performs data and system backups.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.4.1	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The log aggregation tool is configured to alert on suspicious or key events. All alerts are investigated.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.4.2	Logging facilities and log information shall be protected against tampering and unauthorized access.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Log access is restricted to employees who require access to perform their role.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.4.3	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Log access is restricted to employees who require access to perform their role and their access is regularly reviewed and updated where necessary.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.4.4	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Servers are configured to use geographically separate authoritative time sources and re-sync hourly. NTP servers are configured to re-sync production system clocks when the time delay is greater than 1 second.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.5.1	Procedures shall be implemented to control the installation of software on operational systems.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	IT restricts operational software to a list of authorized business and production software and applications.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.6.1	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Vulnerability assessment and threat modeling has been implemented and relevant information is shared with the CISO and other stakeholders.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.6.2	Rules governing the installation of software by users shall be established and implemented.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	IT restricts the installation of new operational software and requires approval.	CISO, CTO, CIO, Legal, IT, and Development.
A.12.7.1	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. Rules governing the installation of software by users shall be established and implemented.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All stakeholders in an upcoming audit are notified and resources and timing allocated.	CISO, CTO, CIO, Legal, IT, and Development.
A.13.1.1	Networks shall be managed and controlled to protect information in systems and applications.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Network configurations are logged and maintained in a revision control system. Network devices are monitored for key operational parameters and alerts are escalated for resolution, if necessary.	CISO, CTO, CIO, Legal, IT, and Development.

A.13.1.2	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Firewalls, intrusion detection systems, and other networking devices are in place to monitor network traffic and security.	CISO, CTO, CIO, Legal, IT, and Development.
A.13.1.3	Groups of information services, users and information systems shall be segregated on networks.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Networks are segregated and managed by IT.	CISO, CTO, CIO, Legal, IT, and Development.
A.13.2.1	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Customer data is classified and handled in accordance with information classification and security policies.	CISO, CTO, CIO, Legal, IT, and Development.
A.13.2.2	Agreements shall address the secure transfer of business information between the organization and external parties.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Vendor Management assesses all relevant new vendors. Confidentiality agreements and security provisions are included in every third party agreement.	CISO, CTO, CIO, Legal, IT, and Development.
A.13.2.3	Information involved in electronic messaging shall be appropriately protected.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Customer data is encrypted at rest and in transit. Remote access sessions into the production environment are encrypted.	CISO, CTO, CIO, Legal, IT, and Development.
A.13.2.4	Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	NDAs are required before sharing any confidential information with third parties. Customer agreements, service-level agreements, and vendor agreements are negotiated before performance or receipt of service. Changes to the standard confidentiality provisions in these contracts require Legal approval.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.1.1	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Technical Security team reviews and approves security related changes prior to implementation in production.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.1.2	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Communication to and from customers is encrypted using TLS 1.2 or the highest level of encryption supported by the client.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.1.3	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Communication to and from customers is encrypted using TLS 1.2 or the highest level of encryption supported by the client.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.1	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Secure Development Lifecycle processes are implemented and adhered to.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.2	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Production application changes are peer reviewed and approved prior to implementation.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.3	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Production application changes are peer reviewed and approved prior to implementation.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.4	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Production application changes are peer reviewed and approved prior to implementation.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.5	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Secure Development Lifecycle processes are implemented and adhered to.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.6	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Secure baseline configurations have been implemented in the development environment.	CISO, CTO, CIO, Legal, IT, and Development.

A.14.2.7	The organization shall supervise and monitor the activity of outsourced system development.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	External outsourced entities are subject to a security due diligence review on a regular cadence in alignment with our Vendor Risk Management framework.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.8	Testing of security functionality shall be carried out during development.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Technical Security team reviews and approves security related changes prior to implementation in production.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.2.9	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	New system requests and system acceptance is documented in JIRA prior to implementation in production.	CISO, CTO, CIO, Legal, IT, and Development.
A.14.3.1	Test data shall be selected carefully, protected and controlled.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Customer data is not used for development or testing purposes. Only aggregated and/or anonymized data is used.	CISO, CTO, CIO, Legal, IT, and Development.
A.15.1.1	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All suppliers and/or third parties with access to systems and/or data are subject to confidentiality and security provisions in contractual agreements.	CISO, CTO, CIO, Legal, IT, and Development.
A.15.1.2	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All suppliers and/or third parties with access to systems and/or data are subject to confidentiality and security provisions in contractual agreements.	CISO, CTO, CIO, Legal, IT, and Development.
A.15.1.3	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	All suppliers and/or third parties with access to systems and/or data are subject to confidentiality and security provisions in contractual agreements.	CISO, CTO, CIO, Legal, IT, and Development.
A.15.2.1	Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Vendor Management assesses each new relevant vendor prior to engagement and as required for the duration of the engagement.	CISO, CTO, CIO, Legal, IT, and Development.
A.15.2.2	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Vendor Management assesses each new relevant vendor prior to engagement and as required for the duration of the engagement.	CISO, CTO, CIO, Legal, IT, and Development.
A.16.1.1	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	A security incident response process has been established that defines the roles and responsibilities for the detection and management of information security incidents.	CISO, CTO, CIO, Legal, IT, and Development.
A.16.1.2	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Information security events are communicated to senior leadership at the Security Management Board and, when appropriate, at the Monthly Business Review meetings.	CISO, CTO, CIO, Legal, IT, and Development.
A.16.1.3	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Crisis Communication Plan establishes communication protocols for system issues, breaches, and security concerns with support from the SOC.	CISO, CTO, CIO, Legal, IT, and Development.
A.16.1.4	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Information security events are assessed by the Technical Security Teamm and CISO office and escalated in accordance with the Security Incident Response process.	CISO, CTO, CIO, Legal, IT, and Development.
A.16.1.5	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Information security events are assessed by the Technical Security Teamm and CISO office and escalated in accordance with the Security Incident Response process.	CISO, CTO, CIO, Legal, IT, and Development.

A.16.1.6	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Incident Response team reviews all information security incidents to identify opportunities to prevent similar incidents in the future.	CISO, CTO, CIO, Legal, IT, and Development.
A.16.1.7	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Information collected that serves as evidence of a security incident is maintained by the CISO team.	CISO, CTO, CIO, Legal, IT, and Development.
A.17.1.1	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Business Continuity Plan and Disaster Recovery Plan have been developed and are maintained by the Chief Information Officer.	CISO, CTO, CIO, Legal, IT, and Development.
A.17.1.2	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Business Continuity Plan and Disaster Recovery Plan have been developed and are maintained by the Chief Information Officer.	CISO, CTO, CIO, Legal, IT, and Development.
A.17.1.3	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Disaster recovery and business continuity testing is performed at least annually and results are reviewed by management.	CISO, CTO, CIO, Legal, IT, and Development.
A.17.2.1	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Fully redundant systems and infrastructure architecture have been implemented in Canada and Ireland.	CISO, CTO, CIO, Legal, IT, and Development.
A.18.1.1	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Legal and Privacy/Compliance maintain all relevant policies and contractual agreements in accordance with all relevant legislation and requirements in the jurisdictions in which the corporation operates.	CISO, CTO, CIO, Legal, IT, and Development.
A.18.1.2	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Legal updates are provided by industry groups, law firms, etc. and the Legal and Compliance teams collaborate to ensure compliance.	CISO, CTO, CIO, Legal, IT, and Development.
A.18.1.3	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Records are maintained in accordance with the data classification schema and data handling and destruction policies.	CISO, CTO, CIO, Legal, IT, and Development.
A.18.1.4	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The Privacy team and the Chief Privacy Officer are accountable for the implementation of the externally facing privacy policy and the employee privacy policy and all privacy related legal matters.	CISO, CTO, CIO, Legal, IT, and Development.
A.18.1.5	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	The encryption policy is reviewed and approved on an annual basis.	CISO, CTO, CIO, Legal, IT, and Development.
A.18.2.1	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	An independent third party auditor is engaged annually to perform a SOC2 audit.	CISO, CTO, CIO, Legal, IT, and Development.
A.18.2.2	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	Security policies are reviewed, approved, and updated by the policy owners as required and at least annually.	CISO, CTO, CIO, Legal, IT, and Development.

A.18.2.3	Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	Yes	Required to satisfy ISMS compliance obligations under one or more of the following: ISO, SOC2, GDPR, CCPA, PIPEDA.	eSentire has an internal audit team and we regularly undertake annual SOC2 and ISO 27001 security assessments.	CISO, CTO, CIO, Legal, IT, and Development.