Clarivate™

17 January 2024

Statement of Applicability- ISO 27001

Contents

Tracking

DOCUMENT OWNER

Name	Title
Scott Breece	Chief Information Security Officer

REVISION HISTORY

Version	Date	Revised By	Changes
1.0	2024-08-21	Information Security Team	Initial Creation
1.01	2024-12-19	Information Security Team	Updated to ISO27001:2022 version

APPROVAL HISTORY

Version	Date	Printed Name	Approvals
1.0	2024-08-21	Scott Breece, Chief Information Security Officer	Approval via email
1.01	2025-01-15	Scott Breece, Chief Information Security Officer	Approval in SAI60

ISO 27001 Statement of Applicability

1. Scope

1.0.1 Covered within the scope of this document are the products and services scope of ISO 27001 Certification under Clarivate group of companies as defined in the ISMS Scope.

2. Purpose

2.0.1 Clarivate proactively strives to maintain security and integrity by following the ISO 27001:2022 standard. This document describes the relevant and applicable controls adopted by Clarivate group of companies to protect confidential data from cyber-attacks, breaches, and unauthorized access. This document serves as a transparent and authoritative reference for internal and external stakeholders, including auditors, management, and clients.

3. ISO 27001: 2022 Annex A Controls

Clause/ Annex A Reference	Control Title	Control Description	Applicability (Clarivate, Innovative, Exlibris)	Implemented (Yes/ No)	Implementation Description
Clause 4	**Context of the organization**				
Clause 4.1	Understanding the organisation and its context	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	Applicable	Yes	External and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome of the ISMS are defined and documented.
Clause 4.2	Understanding the needs and expectations of interested parties	The organization shall determine: a) interested parties that are relevant to the information security management system; and b) the requirements of these interested parties relevant to information security.	Applicable	Yes	Interested parties relevant to the ISMS have been determined, defined and documented.
Clause 4.3	Determining the scope of the information security management system	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	Applicable	Yes	The boundaries and applicability of the ISMS have been determined, and the scope has been documented.
Clause 4.4	Information security management system	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	Applicable	Yes	The ISMS is established, implemented, maintained and continually improved
Clause 5	**Leadership**				
Clause 5.1	Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization. b) ensuring the integration of the information security management system requirements into the organization's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility	Applicable	Yes	Top Management has demonstrated commitment and leadership with respect to the ISMS by; - Setting objectives - Ensuring integration with business processes - Ensuring appropriate resources - Communicating the importance of Info Sec - Ensuring the intended outcomes of the ISMS - Directing and supporting those responsible for Info Sec - Promoting continual improvement
Clause 5.2	Policy	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information. f) be communicated within the organizattion; and g) be available to interested parties, as appropriate	Applicable	Yes	Information Security policy has been established and communicated to all staff within scope. The Information Security policy has been made available to all employees through company intranet.

Clause 5.3	Organizational roles, responsibilities and authorities	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this International Standard; and b) reporting on the performance of the information security management system to top management.	Applicable	Yes	Top Management has assigned responsibility and authority for a) ensuring that the ISMS conforms to the requirements of this International Standard b) reporting on the performance of the information security management system to top management
Clause 6	**Planning**				
Clause 6.1	**Actions to address risks and opportunities**				
Clause 6.1.1	General	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions	Applicable	Yes	Taking considerations from 4.1 and 4.2, the organisation has determined the risks and opportunities that need to be addressed to: a) ensure the ISMS can achieve its intended outcomes b) prevent, or reduce, undesired effects c) achieve continual improvement
Clause 6.1.2	Information security risk assessment	The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) ensures that repeated information security risk assessments produce consistent, valid and comparable results; c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners; d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk; e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analysed risks for risk treatment. The organization shall retain documented information about the information security risk assessment process.	Applicable	Yes	The organization has defined and applied an information security risk assessment process. Information Security team conducts periodic risk assessments in alignment with Information Security Policy.
Clause 6.1.3	Information security risk treatment	The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;	Applicable	Yes	The organization has defined and applied an information risk treatment process and has mapped controls to inherent risks within the SOA

Clause 6.2	**Information security objectives and planning to achieve them**	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be communicated; and e) be updated as appropriate. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible; i) when it will be completed; and j) how the results will be evaluated.	Applicable	Yes	The organisation has established security objectives at relevant functions and levels.
Clause 7	**Support**				
Clause 7.1	Resources	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	Applicable	Yes	The organisation has ensured that the appropriate resources are available to implement and maintain the ISMS.
Clause 7.2	Competence	The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence.	Applicable	Yes	The necessary competence the resources managing the ISMS and affects its information security performance has been determined. Those individuals are evaluated for competence based on appropriate education, training or experience. Where applicable, action has been taken to acquire the necessary competence and evaluate the effectiveness of the actions taken. Appropriate documented information has been retained as evidence of competence
Clause 7.3	Awareness	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	Applicable	Yes	Personnel doing work under the organisation's control are aware of: a) the information security policy b) their contribution to the effectiveness of the ISMS c) the implications of not conforming with the ISMS requirements
Clause 7.4	Communication	The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected	Applicable	Yes	The organisation has determined the need for internal and external communication relevant to the ISMS: a) what to communicate b) when to communicate c) with whom to communicate d) who shall communicate e) the method of communication
Clause 7.5	Documented information				
Clause 7.5.1	General	The organization's information security management system shall include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system	Applicable	Yes	The ISMS includes documents required by the standard and those determined by the organisation as being necessary for the effectiveness of the ISMS.
Clause 7.5.2	Creating and updating	When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number); b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c) review and approval for suitability and adequacy.	Applicable	Yes	When creating and updating documents the organisation ensures that the identification (title, date, author and version) and defined review and approval for ISMS documents has been established to ensure continued suitability.

Clause 7.5.3	Control of documented information	Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	Applicable	Yes	Documents are available and suitable for use and adequately protected from loss or improper use. External documentation relevant to the ISMS has been identified and controlled.
Clause 8	**Operation**				
Clause 8.1	Operational planning and control	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.	Applicable	Yes	The processes needed to meet information security requirements, and to implement the actions determined in 6.1. have been planned, implemented and controlled by the organisation. The organisation has implemented plans to achieve information security objectives determined in 6.2. The organisation keeps documented information to the extent necessary to have confidence that the processes have been carried out as planned. Planned changes are controlled. The consequences of unintended changes are reviewed, taking action to mitigate any adverse effects, as necessary. Outsourced processes have been determined.
Clause 8.2	Information security risk assessment	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.	Applicable	Yes	Information security risk assessments occur at planned intervals or when significant changes are proposed or occur. Documented information is retained as evidence of the results of the information security risk assessments.
Clause 8.3	Information security risk treatment	The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	Applicable	Yes	The Information security risk treatment plan has been implemented. Documented information is retained as evidence of the information security risk treatment.
Clause 9	**Performance Evaluation**				
Clause 9.1	Monitoring, measurement, analysis and evaluation	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; c) when the monitoring and measuring shall be performed; d) who shall monitor and measure; e) when the results from monitoring and measurement shall be analyzed and evaluated; and f) who shall analyse and evaluate these results. The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	Applicable	Yes	The Information security performance and the effectiveness of this ISMS is evaluated and reviewed by the management. What needs to be measured, what methods are used, when and by who results are measured and analyzed have been defined. Documented information has been retained as evidence of the monitoring and measurement results.
Clause 9.2	Internal Audit	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard; b) is effectively implemented and maintained. The organization shall: c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits; d) define the audit criteria and scope for each audit; e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; f) ensure that the results of the audits are reported to relevant management; and g) retain documented information as evidence of the audit programme(s) and the audit results	Applicable	Yes	An audit programme has been planned, established, implemented and maintained including the frequency, methods, responsibilities and planning requirements The results of the audits are reported to relevant management; and Documented information has been retained as evidence of the audit programme(s) and the audit results.

Clause 9.3	Management Review	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives; d) feedback from interested parties; e) results of risk assessment and status of risk treatment plan; and f) opportunities for continual improvement. The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.	Applicable	Yes	Top management reviews the organisation's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
Clause 10	**Improvement**				
Clause 10.1	Monitoring, measurement, analysis and evaluation	When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the non-conformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of: f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action	Applicable	Yes	When non-conformity occurs, the organisation reacts to the nonconformity, evaluates the need for action to eliminate the causes of nonconformity in order that it does not recur elsewhere, implements any action needed, reviews the effectiveness of any corrective action taken; and makes changes to the information security management system, if necessary. Documented information is retained as evidence of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action.
Clause 10.2	Continual Improvement	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system	Applicable	Yes	The organisation has continually improved the suitability, adequacy and effectiveness of the ISMS.
ANNEX A CONTROLS					
A.5	**Organizational Controls**				
A.5.1	Policies for Information Security	The Information Security policy shall be defined and approved by senior management. It shall be published, communicated to and acknowledged by all employees and relevant stakeholders, and reviewed at planned intervals and if significant changes occur.	Applicable	Yes	The organisation has an established Information Security Policy document that states the management intent to maintain a secure information-processing environment and to protect information from all threats, whether internal or external, deliberate or accidental. The policy is communicated to employees through company intranet. Security awareness trainings and acknowledgements taken from the employees.
A.5.2	Information security roles and responsibilities	The information security roles and responsibilities shall be established, documented, and allocated according to organization's needs.	Applicable	Yes	Information Security Policy is reviewed regularly (at least annually) to ensure it remains appropriate for the business. This policy is immediately reviewed whenever there is any significant

					change, which may have impact on information security.
A.5.3	Segregation of duties	Conflicting duties and areas of responsibility should be segregated to reduce risk of fraud, error and bypassing of information.	Applicable	Yes	The organisation has defined security responsibilities at an organisation level detailing specific responsibility to be performed by the Security groups and personnel.
A.5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established security policy, topic-specific policies, and procedures of the organization.	Applicable	Yes	All key roles and responsibilities have adequate segregation of duties designed while assigning them to protect against negligent or deliberate misuse of data or services and to reduce opportunity for unauthorized modification to the systems.
A.5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities	Applicable	Yes	Contact details of various emergency services and relevant authorities is maintained.
A.5.6	Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Applicable	Yes	Specialist advice on security is sought from either internal or external advisors when requisite expertise is not available in-house. Additionally, membership of security groups and industry forums including CISA is in place for periodic updates on emerging security threats and updates on security standards.
A.5.7	Threat Intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Applicable	Yes	Information Security is addressed as part of project management and security controls are identified as part of the business requirements for new information systems or enhancements to existing information systems and security is part of the project.
A.5.8	Information Security in Project Management	Information security shall be integrated into project management.	Applicable	Yes	An established mobile device standard is in place which defines security requirements while using mobile computing devices and safeguards for the risk introduced by it.
A.5.9	Inventory of information and other associated assets	An Inventory of information and other associated assets, including owners, shall be established and maintained.	Applicable	Yes	Teleworking Standard has been established which defines security requirements and controls to be implemented along with best practices that must be followed by employees while working remotely.
A.5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedure for handling information and other associated assets shall be identified, documented, and implemented.	Applicable	Yes	In accordance with relevant laws and regulations, adequate background verification checks are performed while recruiting an individual as permanent staff to ensure the authenticity of the individual and to reduce the possibility of threat to critical information assets.
A.5.11	Return of assets	Personnel and other interested parties as appropriate shall return all organization's assets in their possession upon change or termination of their employment, contract or agreement.	Applicable	Yes	Terms and conditions of employment are incorporated in the joining documents for employees administered by Human Resources Department. All employees are required to sign an Employment agreement at the time of their appointment, which contains clauses related to non-disclosure of confidential information, information security, compliance to applicable laws and code of ethics.
A.5.12	Classification of information	Information shall be classified according to the information security needs of the organization and shall be based on confidentiality, integrity, availability, and relevant interested party requirements.	Applicable	Yes	Management responsibilities include that the Information Security policies are always kept up to date and the employees and contractors are aware of their information security responsibilities which are to be acknowledged by them on a regular basis.

A.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 organization	Applicable	Yes	New employees are imparted information security awareness training to educate them adequately on security responsibilities and security best practices to protect information assets. Also, annual Information Security policy awareness training is conducted to obtain acknowledgement of security roles and responsibilities by all employees and contractors as defined in the organisation's Information Security Policy and standards.
A.5.14	Information transfer	Information transfer rules, procedures, or agreements should be developed for all types of transfer facilities within the organisation and between other parties.	Applicable	Yes	A formal Security Enforcement standard is in place to address non-compliance and violations to organisation's Information Security policy and standards.
A.5.15	Access Control	Access to all critical systems will be granted by the IT Department based on job role and function, and access rights will be reviewed at scheduled intervals with any necessary changes made immediately.	Applicable	Yes	Information Security responsibilities that remain valid even after termination or change of employment are part of the employment contract which is signed at the time of joining.
A.5.16	Identity management	The organization shall establish a process that covers the approval for creating, revoking and deletion of unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.	Applicable	Yes	The organisation departments maintain an inventory of information assets to ensure that the assets are effectively identified and protected.
A.5.17	Authentication Information	Allocation and management of authentication shall be controlled by a management process, including advising on the appropriate handling of authentication information.	Applicable	Yes	The ownership of the information asset is defined and maintained
A.5.18	Access rights	Access rights to information and other associated assets shall be established, reviewed, modified and removed in accordance with the organisation's topic-specific policy and rules for access control.	Applicable	Yes	Employees are required to read and acknowledge organisation's Information Security Policy and Standards including terms of acceptable use of assets as part of the annual Information Security policy awareness training. Acceptable use Standard includes measures to ensure that company assets, supporting systems and data stored or transmitted on them is utilized by users in a professional and responsible manner.
A.5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Applicable	Yes	The employee termination process involves revocation of system permissions/access rights and return of company assets in a timely manner by employees, contractors and third-party users upon termination of employment contract/ agreement.
A.5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Applicable	Yes	Data classification, handling and Retention standard assign levels of classification to information and assets to indicate the degree of protection required basis their business criticality in order to protect them appropriately.
A.5.21	Managing information security in the ICT supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Applicable	Yes	Information assets are labelled as per the data classification scheme and handled as per the provisions of Data classification, handling and Retention standard.
A.5.22	Monitor, review, and change management of supplier services	The organization shall regularly monitor, review, evaluate, and manage change in supplier information security practices and service delivery.	Applicable	Yes	Procedures for handling assets have been developed and implemented in accordance with the information classification scheme adopted by the organisation.
A.5.23	Information security for use of cloud services	Processes for acquisition, use, management, and exit from cloud services shall be established in accordance with the organization's information security requirements.	Applicable	Yes	Procedures are defined for management of removable computer media. Backup tapes tape movement. In addition,
A.5.24	Information security incident management, planning, and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities.	Applicable	Yes	Media storing information is disposed securely to prevent unauthorized access. Procedures and methods are established for secure disposal of media.

A.5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorised as information security incidents.	Applicable	Yes	Assets physical and electronic are protected during transportation by the organisation.
A.5.26	Response to information security Incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Applicable	Yes	Access to information and information systems is controlled based on business and security requirements. A clearly defined Access Control Standard is in place.
A.5.27	Learning from information security incidents	. Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Applicable	Yes	Access to network and network services for users are provided based on principle of need-to-know, need-to-do, least-privilege and for valid business justification only.
A.5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.	Applicable	Yes	The organisation has an established user creation and deletion for the information systems basis a valid business approval.
A.5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Applicable	Yes	The organisation has a formal user access provisioning process to assign or revoke access from the various information systems.
A.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.	Applicable	Yes	Allocation of privileged access rights is restricted and controlled through a formal authorization process and is based on a valid business justification.
A.5.31	Identification of legal, statutory, regulatory, and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and approach to meet these requirements should be identified, documented, and kept up to date.	Applicable	Yes	The organisation has a formal process for allocation of secret authentication information through defined process.
A.5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Applicable	Yes	There is a defined process of performing access rights review on the information systems on a regular frequency.
A.5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Applicable	Yes	The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract /agreement, and adjusted upon change of role.
A.5.34	Privacy and protection of PII	Organizations should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and contractual requirements.	Applicable	Yes	Password management guidelines are defined, and users are advised on secure password handling techniques.
A.5.35	Independent review of information security	Organization's approach to managing information security and its implementation include people, processes and the technologies should be reviewed independently at planned intervals, or when significant changes occur.	Applicable	Yes	Access to information systems and applications is based on need-to-know and on the principle of least privilege
A.5.36	Compliance with policies, rules, and standards for information security	Compliance with the organization information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Applicable	Yes	User authentication to information systems is via a unique username and password.
A.5.37	Documented operating procedures	Operating procedures for information processing should be documented and made available to personnel who need them.	Applicable	Yes	Password control is enabled via group policy of the domain or through individual information systems configuration.
A.6	**People Controls**				
A.6.1	Screening	Background verification checks on all candidates to personnel should be carried out prior to joining an organization 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.	Applicable	Yes	The organisation has an established an Encryption Standard which details the process for encryption of data in rest and in motion along with the key management process in place.

A.6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Applicable	Yes	The organisation has an established an Encryption Standard detailing the key management process followed during the lifecycle.
A.6.3	Information security awareness, education, and training	Personnel and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic specific policies and procedures, as relevant for their job function.	Applicable	Yes	Information processing facilities supporting critical or sensitive business activities are physically protected against unauthorized access, damage, and interference.
A.6.4	Disciplinary Process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security violation.	Applicable	Yes	Secure areas Are identified within the premises and have additional security mechanisms such as proximity-based access control systems / key readers are used to ensure that with restricted access.
A.6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Applicable	Yes	Office premises are adequately secured through card-based access controls to restrict the movement of unauthorized personnel and ensuring having visitor management procedures.
A.6.6	Confidentiality or non-disclosure agreement	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties.	Applicable	Yes	Office premises are protected from damage from fire, flooding, explosion, civil unrest and other forms of natural or man-made threats using physical security controls. Heat / Smoke / Fire detection and suppression system are in place in addition to emergency evacuation procedures.
A.6.7	Remote working	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties.	Applicable	Yes	The access to Secure areas requires authentication through a proximity / key reader access control system. The system is electronically designed to allot, modify, and remove the access to various zones and people depending upon their role in the organization.
A.6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Applicable	Yes	An isolated delivery and loading area (for supplies and equipment deliveries) is in place for the office premises to reduce the opportunity for unauthorized access to secure areas.
A.7	**Physical Controls**				
A.7.1	Physical security perimeters	To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.	Applicable	Yes	Information processing equipment are sited and protected in secure areas to reduce risks from environmental hazards and to minimize the opportunity of unauthorized access. Suitable environment controls like HVAC, Adequate power supply, Heat and Smoke Detectors, Fire are installed as per industry standard best practices.
A.7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Applicable	Yes	Information processing equipment is protected against power failures, voltage surges, spikes and other disruptions caused by failure in supporting utilities. All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning are implemented for the systems they are supporting.
A.7.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities should be designed and implemented.	Applicable	Yes	Cabling is done based on the international standards and best practices be protected from interception, interference or damage.
A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Applicable	Yes	Critical equipment is under warranty and support agreements. Equipment is maintained as per manufacturer's specifications.
A.7.5	Protecting against physical and environmental threats	Protection against physical and environment threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Applicable	Yes	Movement of information processing equipment, storage media or software to off-site location or for maintenance activities is carried out after obtaining appropriate authorization. material movements are monitored and only allowed after valid business justification and approvals.

A.7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Applicable	Yes	IT equipment is sent outside the organization through a formal approval process. Employees using laptops and mobile computing devices are required to follow the Teleworking standard and Clear Desk Standard for usage of information assets outside office premises and adequate security controls are in place to protect information in transit or if using a different location. Only authorized mobile computing device are allowed to connect to the organisation Global Network to minimize security risks and to protect company and customer data.
A.7.7	Clear desk and clear screen	Clear desk rules for papers, removal storage media, and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Applicable	Yes	The organisation has adopted industry standard media disposal techniques. Secure disposal is applicable to all assets like hard drives and removable media drives including backup tapes.
A.7.8	Equipment sitting and protection	Equipment shall be sited securely and protected.	Applicable	Yes	Workstations are configured for lockout after a defined period of inactivity. In addition, employees using laptops and mobile computing devices are required to follow the Teleworking standard and Clear Desk Standard for usage of information assets outside office premises to to protect information assets that contain confidential information.
A.7.9	Security of assets off-premises	Off-site assets shall be protected.	Applicable	Yes	Clear Desk Standard has been established that includes the measures to prevent unauthorized access, loss and damage to the information in electronic, paper documents and electronic media form during and after normal working hours. Paper outputs are disposed of through shredding bins and paper shredders.
A.7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation, and disposal in accordance with the organization's classification scheme and handling requirements.	Applicable	Yes	Standard operating procedures have been established for systematic and structured approach to manage business operations in a secure manner.
A.7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Applicable	Yes	Changes to the information systems which includes changes to business applications, network, telecom equipment, software and infrastructure procedures, are subject to change management process with adequate approvals and documentation.
A.7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception.	Applicable	Yes	Information processing facilities are regularly monitored to ensure continuous availability of capacity to meet future business requirements.
A.7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure the Confidentiality, integrity and availability of information.	Applicable	Yes	The organisation maintains separate development, test and production environments for the various business applications and products with dedicated access controls to restrict unauthorized transfer of changes.
A.7.14	Secure disposal or re-use of equipment	Equipment shall be maintained correctly to ensure the Confidentiality, integrity and availability of information.	Applicable	Yes	Malware protection software is installed on all workstations & servers. Virus definitions are updated on a periodical basis. In addition, Security patches are installed to prevent against known vulnerabilities.
A.8	**Technological Controls**				
A.8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices shall be protected.	Applicable	Yes	Backup of the data on applications, servers and network configurations are taken on the regular basis. Tapes are regularly sent to offsite location.
A.8.2	Privileged access rights	Information stored on, processed by or accessible via user endpoint devices shall be protected.	Applicable	Yes	Logging is enabled on Critical servers and Network /Security devices. Alerts are configured in SIEM which are

					reviewed and actioned upon across Infrastructure and Applications.
A.8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Applicable	Yes	Logs are archived and stored with restricted accesses to personnel who are responsible for monitoring the logs.
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Applicable	Yes	Administrator and operator logging is enabled and is reviewed on a need basis.
A.8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the tpoic-specific policy on access control.	Applicable	Yes	Information systems within the organisation are synchronized to a single reference time source.
A.8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Applicable	Yes	The organisation has defined a formal process for installation of any software on operational systems to ensure their integrity is not hampered or compromised.
A.8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Applicable	Yes	The organisation's Information Security team continuously monitors forums for known vulnerabilities and also conducts internal and external vulnerability assessment in order to identify and remediate them.
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, organization's exposure to such vulnerabilities shall be evaluated and appropriate measures should be taken.	Applicable	Yes	The organisation has defined a formal process for ensuring only authorised software is installed on systems after appropriate approvals.
A.8.9	Configuration management	Configurations, including security cofigurations of software, hardware, services, and networks shall be established, documented, implemented, monitored, and reviewed.	Applicable	Yes	Internal audits are carried out at periodic intervals to ensure compliance to company security policies and standard operating procedures and audit reports, corrective actions and remediation plans maintained.
A.8.10	Information deletion	Information stored in information systems, devices, or in any storage media shall be deleted when no longer required.	Applicable	Yes	Company network is adequately protected at perimeter level and has been logically segmented into various security zones with defined rules of access.
A.8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control, other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Applicable	Yes	Networking Services are provisioned, managed and monitored. Unnecessary services are disabled by default.
A.8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks, and any other devices that process, store or transmit sensitive information.	Applicable	Yes	Network has been logically segmented into various security zones with defined rules of access.
A.8.13	Information backup	. Backup copies of information, software, and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Applicable	Yes	Controls are implemented to minimize the risks associated with Information exchange through different types of channels. File Transfer Standard has been established for business approved mechanisms for data transfer and controls have been implemented to meet security requirements defined in company security policies.
A.8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Applicable	Yes	Agreements and handling procedures have been established consistent with the confidentiality of the information and software. Exchange agreements incorporate confidentiality terms and conditions for information and software exchange and responsibilities and liabilities for loss or damage have been defined. Third Party Connectivity controls are in place for establishing Third Party connections between the organisation and external parties for the exchange of information.
A.8.15	Logging	Logs that record activities, exceptions, faults, and other relevant events shall be produced, stored, protected, and	Applicable	Yes	Appropriate controls have been established for security of electronic messages to minimize the risk of

		analysed.			messages being read by unauthorized persons, intercepted or modified.
A.8.16	Monitoring services	Networks, systems, and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Applicable	Yes	Employees and contractors are required to sign confidentiality agreements which contains clauses related to non-disclosure of confidential information, information security, compliance to applicable laws and code of ethics. Third-party users or contract staff are also required to sign Non-Disclosure Agreement (NDAf) or confidentiality agreements.
A.8.17	Clock synchronisation	The clocks of information processing systems used by the organization shall be synchronised to approved time sources	Applicable	Yes	Security requirements are considered when new Business systems/ Information systems are introduced into the Organization or when there are changes made to existing business systems/ information systems. Where changes are made, these are recorded and documented.
A.8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Applicable	Yes	The organisation has defined encryption standard and key management practices which requires the application related communication to be encrypted over public networks.
A.8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Applicable	Yes	The organisation has defined encryption and key management practices which requires all the application related communication to be encrypted.
A.8.20	Network controls	Networks and network devices shall be secured, managed, and controlled to protect information in systems and applications.	Applicable	Yes	The organisation has defined guidelines for secure development of applications to build up a secure service, architecture, software and system.
A.8.21	Security of network services	Security mechanisms, service levels, and service requirements of network services shall be identified, implemented and monitored.	Applicable	Yes	Changes to the operating information systems environment, which includes changes to servers, network and telecom equipment, software, operational programs and procedures, are subject to strict change control procedures and all the changes are documented, tested and authorized before being implemented.
A.8.22	Segregation in networks	Security mechanisms, service levels, and service requirements of network services shall be identified, implemented and monitored.	Applicable	Yes	Applications are tested during any upgrade or change in the operating system to ensure that applications function efficiently and effectively to meet business requirements. All the changes to the operating system and application integration changes are subject to formal change control procedures.
A.8.23	Web filtering	Access to external websites shall be managed to reduced exposure to malicious content.	Applicable	Yes	Software supplied by trusted vendor is deployed in the company environment and no modifications are performed to software packages by IT Support team.
A.8.24	Use of cryptography	Rules for effective use of cryptography, including cryptographic key management, shall be defined and implemented by the IT security team and rotated every 12 months and shall be stored in a secure, tamper-proof environment.	Applicable	Yes	Principles for engineering secure systems have been established, documented, maintained and applied to any information system implementation efforts.
A.8.25	Secure development lifecycle	Rules for secure development of software and systems shall be established and applied.	Applicable	Yes	The organisation has defined guidelines to establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
A.8.26	Application security requirements	Information security requirements shall be identified, specified, and approved when developing or acquiring applications.	Not Applicable	No	The organisation products are developed by an inhouse dedicated team of software developers and application security experts. The organisation shall collaborate with trusted third-party vendors in regard the

					software development and monitor the activity of outsourced system development.
A.8.27	Secure system architecture and engineering principles	Principles for engineering systems shall be established, documented, maintained and applied to any information systems development activities.	Applicable	Yes	Software Development and QA teams perform testing for enhancements and product releases to identify vulnerabilities in the code being transferred to production environment.
A.8.28	Secure coding	Secure coding principles shall be applied to software development.	Applicable	Yes	Systems confirming to industry standard best practices and from reputed vendors are procured. Systems are validated through user acceptance / security testing before being incorporated into production environment.
A.8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development lifecycle.	Applicable	Yes	Production data is not used for testing purposes.
A.8.30	Outsourced development	The organization shall direct, monitor, and review the activities related to outsourced system development.	N/A	Yes	The organization products are developed by an inhouse dedicated team of software developers and application security experts. The organization shall collaborate with trusted third-party vendors in regard to the software development and monitor the activity of outsourced system development.
A.8.31	Separation of development, test, and production environments	Rules for the secure development of software and systems shall be established and applied.	Applicable	Yes	The organisation Master Service Agreement incorporates confidentiality terms and conditions, security controls, service definitions, and delivery levels in service delivery agreements. These agreements include security requirements and appropriate controls required to be in place. This also includes the security requirements for third party access for the protection of the company network and information assets.
A.8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Applicable	Yes	Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.8.33	Test information	Test information shall be appropriately selected, protected and managed.	Applicable	Yes	Periodic reviews are conducted by the relevant teams based on the established Service Level Agreements to check the efficiency of the service and to report deviations.
A.8.34	Protection of information systems during audit and testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Applicable	Yes	Any changes to Third Party Services being provided are analysed and the Impact is determined before changes are accepted and implemented.

Appendix

4. References

Applicable ISO 27001 Certificates: **https://clarivate.com/trust-center/security-compliance/**