

Document Name: ISO27001/27017/27701 Statement of Applicability
Company Name: OneTrust, LLC

Version History

Version	Date	Prepared/Updated By
1.0	9/18/23	Chih-Shen Hsieh Maria Golubenko
1.1	11/16/23	Maria Golubenko
1.2	4/26/24	Chih-Shen Hsieh Daniel Chen Maria Golubenko
1.3	4/23/25	Daniel Chen Maria Golubenko

Summary of Changes	Approved By
Reviewed and updated for ISO 27001:2022 and ISO 27701:2019.	Kevin Liu
Updated ISO 27701 for justification, and N/A for PIMS - A.7.2.7 - Joint Data Controller	Linda Thielova
Updated for ISO 27017:2015	Tim Mullen Adrienne Canter
Annual review performed; no scope or control applicability changes; minor updates made to applicability justification description for both IMS and PIMS.	Tim Mullen Adrienne Canter Angela Potter Linda Thielova

Control Name	Control Description	Control Applicability (27001)
ISO 27001:2022 (ISMS)		
5.1 - Policies for Information Security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes
5.2 - Information Security Roles and Responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization's needs.	Yes
5.3 - Segregation of Duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes
5.4 - Management Responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes
5.5 - Contact with Authorities	The organization shall establish and maintain contact with relevant authorities.	Yes
5.6 - Contact with Special Interest Groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes
5.7 - Threat Intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	Yes
5.8 - Information Security in Project Management	Information security shall be integrated into project management.	Yes

5.9 - Inventory of Information and Other Associated Assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes
5.10 - Acceptable Use of Information and Other Associated Assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes
5.11 - Return of Assets	Personnel and other interested parties, as appropriate, shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes
5.12 - Classification of Information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes
5.13 - Labelling of Information	An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes
5.14 - Information Transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes
5.15 - Access Control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Yes
5.16 - Identity Management	The full life cycle of identities shall be managed.	Yes
5.17 - Authentication Information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Yes

5.18 - Access Rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes
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 suppliers' products or services.	Yes
5.20 - Addressing Information Security within Supplier Agreements	Relevant information security requirements shall be established and agreed upon with each supplier based on the type of supplier relationship.	Yes
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.	Yes
5.22 - Monitoring, Review and Change Management of Supplier Services	The organization shall regularly monitor, review, evaluate and manage changes in supplier information security practices and service delivery.	Yes
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.	Yes
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.	Yes
5.25 - Assessment and Decision on Information Security Events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Yes
5.26 - Response to Information Security Incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes

5.27 - Learning from Information Security Incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Yes
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.	Yes
5.29 - Information Security during Disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes
5.30 - ICT Readiness for Business Continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes
5.31 - Legal, Statutory, Regulatory and Contractual Requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes
5.32 - Intellectual Property Rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes
5.33 - Protection of Records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes
5.34 - Privacy and Protection of PII	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes
5.35 - Independent Review of Information Security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Yes
5.36 - Compliance with Policies, Rules and Standards for Information Security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Yes

5.37 - Documented Operating Procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes
6.1 - Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the 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.	Yes
6.2 - Terms and Conditions of Employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes
6.3 - Information Security Awareness, Education and Training	Personnel of the organization 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.	Yes
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 policy violation.	Yes
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.	Yes
6.6 - Confidentiality or Non-Disclosure Agreements	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.	Yes

6.7 - Remote Working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes
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.	Yes
7.1 - Physical Security Perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes
7.2 - Physical Entry	Secure areas shall be protected by appropriate entry controls and access points.	Yes
7.3 - Securing Offices, Rooms and Facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Yes
7.4 - Physical Security Monitoring	Premises shall be continuously monitored for unauthorized physical access.	Yes
7.5 - Protecting Against Physical and Environmental Threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Yes
7.6 - Working in Secure Areas	Security measures for working in secure areas shall be designed and implemented.	Yes
7.7 - Clear Desk and Clear Screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Yes
7.8 - Equipment Siting and Protection	Equipment shall be sited securely and protected.	Yes
7.9 - Security of Assets Off-Premises	Off-site assets shall be protected.	Yes
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.	Yes

7.11 - Supporting Utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes
7.12 - Cabling Security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Yes
7.13 - Equipment Maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes
7.14 - Secure Disposal or Re-Use of Equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.	Yes
8.1 - User Endpoint Devices	Information stored on, processed by or accessible via user endpoint devices shall be protected.	Yes
8.2 - Privileged Access Rights	The allocation and use of privileged access rights shall be restricted and managed.	Yes
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.	Yes
8.4 - Access to Source Code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Yes
8.5 - Secure Authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes
8.6 - Capacity Management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes

8.7 - Protection against Malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Yes
8.8 - Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Yes
8.9 - Configuration Management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes
8.10 - Information Deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes
8.11 - Data Masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes
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.	Yes
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.	Yes
8.14 - Redundancy of Information Processing Facilities	Information processing facilities shall be implemented with redundancy sufficient to meet the availability requirements.	Yes
8.15 - Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.	Yes
8.16 - Monitoring Activities	Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	Yes

8.17 - Clock Synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes
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.	Yes
8.19 - Installation of Software on Operational Systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes
8.20 - Networks Security	Networks and network devices shall be secured, managed and controlled to protect the information in systems and applications.	Yes
8.21 - Security of Network Services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes
8.22 - Segregation of Networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Yes
8.23 - Web Filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes
8.24 - Use of Cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes
8.25 - Secure Development Life Cycle	Rules for the secure development of software and systems shall be established and applied.	Yes
8.26 - Application Security Requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes
8.27 - Secure System Architecture and Engineering Principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Yes

8.28 - Secure Coding	Secure coding principles shall be applied to software development.	Yes
8.29 - Security Testing in Development and Acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Yes
8.30 - Outsourced Development	The organization shall direct, monitor and review the activities related to outsourced system development.	Yes
8.31 - Separation Of Development, Test and Production Environments	Development, testing and production environments shall be separated and secured.	Yes
8.32 - Change Management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes
8.33 - Test Information	Test information shall be appropriately selected, protected and managed.	Yes
8.34 - Protection of Information Systems During Audit Testing	Audit tests and other assurance activities involving the assessment of operational systems shall be planned and agreed upon between the tester and appropriate management.	Yes
ISO 27017:2015 (code of practice for information security controls). OneTrust is Cloud Service Customer		
CLD.6.3.1 - Shared Roles and Responsibilities in Cloud Computing	Shared roles and responsibilities for information security in the use of the cloud service shall be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.	
CLD.8.1.5 - Removal of Cloud Service Customer Assets	Assets of the cloud service customer that are on the cloud service provider's premises shall be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	
CLD.9.5.1 - Segregation in Virtual Computing Environments	A cloud service customer's virtual environment running on a cloud service shall be protected from other cloud service customers and unauthorized persons.	

<p>CLD.9.5.2 - Virtual Machine Hardening</p>	<p>Virtual machines in a cloud computing environment shall be hardened to meet business needs.</p>	
<p>CLD.12.1.5 - Administrator's Operational Security</p>	<p>Procedures for administrative operations of a cloud computing environment shall be defined, documented and monitored.</p>	
<p>CLD.12.4.5 - Monitoring of Cloud Services</p>	<p>The cloud service customer shall have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.</p>	
<p>CLD.13.1.4 - Alignment of Security Management for Virtual and Physical Networks</p>	<p>Upon configuration of virtual networks, consistency of configurations between virtual and physical networks shall be verified based on the cloud service provider's network security policy.</p>	

Control Applicability (27017 Cloud Service Customer)	Control Applicability (27017 Cloud Service Provider)	Implemented
Yes	Yes	Yes
Yes	Yes	Yes
		Yes
		Yes
Yes	Yes	Yes
		Yes
		Yes
Yes	Yes	Yes

Yes	Yes	Yes
		Yes
		Yes
		Yes
Yes	Yes	Yes
		Yes
Yes	(no additional implementation guidance)	Yes
(no additional implementation guidance)	Yes	Yes
Yes	Yes	Yes

(no additional implementation guidance)	Yes	Yes
Yes	(no additional implementation guidance)	Yes
Yes	Yes	Yes
(no additional implementation guidance)	Yes	Yes
		Yes
		Yes
Yes	Yes	Yes
		Yes
		Yes

		Yes
Yes	Yes	Yes
		Yes
		Yes
Yes	Yes	Yes
Yes	Yes	Yes
Yes	Yes	Yes
		Yes
Yes	Yes	Yes
		Yes

		Yes
		Yes
		Yes
Yes	Yes	Yes
		Yes
		Yes
		Yes

		Yes
Yes	Yes	Yes
		Yes
		Yes
		Yes
		Yes
		Yes
		Yes
		Yes
		Yes
		Yes
		Yes
		Yes
		Yes

		Yes
		Yes
		Yes
No	No	Yes
		Yes
Yes	Yes	Yes
Yes	Yes	Yes
		Yes
		Yes
Yes	Yes	Yes

		Yes
Yes	Yes	Yes
		Yes
		Yes
		Yes
		Yes
Yes	Yes	Yes
		Yes
Yes	Yes	Yes
		Yes

Yes	No	Yes
Yes	No	Yes
		Yes
		Yes
		Yes
Yes	Yes	Yes
		Yes
Yes	Yes	Yes
Yes	Yes	Yes
		Yes
		Yes

		Yes
Yes	(no additional implementation guidance)	Yes
		Yes
		Yes
Yes	Yes	Yes
		Yes
		Yes
and Cloud Service Provider.		
Yes	Yes	Yes
Yes	Yes	Yes
(no additional implementation guidance)	Yes	Yes

Yes	No	Yes
Yes	Yes	Yes
Yes	Yes	Yes
(no additional implementation guidance)	Yes	Yes

Justification (Applicable/ Not Applicable)
<p>To ensure expectations and requirements of organization's Information Security Management System (ISMS) are clearly defined and communicated to all employees and relevant external parties. In addition, this is relevant in order to demonstrate Management's commitment with the organization's ISMS.</p>
<p>This control is applicable as it ensures that basic roles and responsibilities to meet the organization's ISMS requirements are defined and allocated. In doing so, this reduces the risk of unauthorized actions due to misunderstandings and lack of <u>accountability</u>.</p>
<p>This control is applicable to reduce opportunities for unauthorized or unintentional modification to information systems. Also, to control risks and enable the organization to detect and correct errors made by employees and contractors.</p>
<p>This control is applicable to execute the ISMS and guide on how to secure information of company and its customers.</p>
<p>This control is applicable as it ensures a prompt response from relevant authorities in the event of an incident when such response is required. Also, to ensure incidents are reported and responded in a timely manner.</p>
<p>This control is applicable to keep personnel updated on the relevant information security trends and threats to secure the organization's assets. Also, required to receive early warnings of security alerts, advisories, and patches about security attacks and information systems vulnerabilities.</p>
<p>This control is applicable to produce consistent threat intelligence information and facilitate an increased security posture. Also, required to provide awareness of the organization's threat environment so that the appropriate <u>mitigation actions can be taken</u>.</p>
<p>This control is applicable to ensure security commitments are embedded in the organization by design and not an afterthought. Also, to enable the outcomes of projects to be <u>delivered in a secure state</u>.</p>

This control is applicable to keep track of information assets used in the organization in order to protect the relevant assets, identify technology gaps, continuous maintenance and track asset lifecycle. Also, to ensure owners and stakeholders take responsibility in securing information assets they are responsible for

This control is applicable to define and implement acceptable use criteria for organizational assets and to protect assets from unauthorized use.

This control is applicable to prevent any leakage, loss, and unauthorized access to assets, including organization and its customer's information after termination of employment or contract.

This control is applicable to enable appropriate level of protection on the information assets based on its criticality and sensitivity level.

This control is applicable to guide on how to label/classify information assets based on its criticality and sensitivity level.

This control is applicable to describe the process to be followed in the exchange of information and control the flow of information in a secure manner between the organization and internal/external entities. Also, to secure and protect information in transit between the organization and its internal/external entities

This control is applicable to minimize risks of unauthorized access to information assets owned by organization as well as to customer data.

This control is applicable to guide users on the process of granting and revoking access based on job needs in order to prevent any unauthorized access to information systems.

This control is applicable to ensure that authentication to information systems is properly restricted and managed in order to prevent unauthorized access.

This control is applicable to guide users on the process of granting and revoking access based on job needs in order to prevent any unauthorized access to information systems.

This control is applicable to mitigate the security risks associated with suppliers' access to the organization's information assets as the organization uses service providers to support its services. Also, required to ensure that organization's security commitments are agreed by suppliers to ensure accountability.

This control is applicable to mitigate the security risks associated with suppliers' access to the organization's information assets as the organization uses service providers to support its services. Also, to ensure that there is no misunderstanding between the organization and the suppliers regarding both parties' obligations to fulfil relevant information security requirements.

This control is applicable to mitigate the security risks associated with suppliers' access to the organization's information assets as the organization uses service providers to support its services. Also, to ensure that there is no misunderstanding between the organization and the suppliers regarding both parties' obligations to fulfil relevant information security requirements.

This control is applicable to ensure that information security requirements defined in the agreements with the suppliers are adhered by the suppliers.

This control is applicable as the organization uses cloud computing services as an SaaS/IaaS/PaaS provider for the application, network, and system infrastructure. This control is required in order specify and manage information security for the use of cloud services.

This control is applicable to ensure an orderly and effective response to reported information security events and weaknesses as well as to ensure accountability of roles and responsibilities when addressing information security incidents.

This control is applicable to ensure that appropriate assessment of security event should be carried out prior to classifying an incident as security incident.

This control is applicable for effective handling of information security incidents in a timely manner with respect to the confidentiality, integrity and availability of the data of the organization and its customers.

<p>This control is applicable to evaluate lessons learned from incidents to prevent future occurrences and to continually improve its information security practices.</p>
<p>This control is applicable in order to perform root cause analysis of security incidents to prevent recurrence as well as for the purposes of any legal/disciplinary action (if applicable) following an information security incident.</p>
<p>This control is applicable to ensure structured and managed approach to restoring business processes so that information security controls continue to operate during adverse situations.</p>
<p>This control is applicable to ensure the availability of the organization's information and other associated assets during disruption.</p>
<p>This control is applicable as it manages the risk related to the breach of applicable laws and regulations as well as contractual requirements due to unawareness.</p>
<p>This control is applicable as it protects the Intellectual Property Rights (IPR) owned by the organization, as well as ensuring that the organization is not in breach of IPRs that may represent a risk to the organization's management (reputational, financial risks and penalties).</p>
<p>This control is applicable as it manages the risk of loss, destruction, and falsification of records, as well as ensuring compliance with applicable legislative, regulatory, contractual, and business requirements.</p>
<p>This control is applicable as it manages the risk of unauthorized disclosure of PII and limits the impact of potential lawsuits on the organization.</p>
<p>This control is applicable as it ensures that the ISMS is effective and compliant with relevant legislative, regulatory, contractual, and business requirements. As well, it ensures continual improvement to the organization's information security practices.</p>
<p>This control is applicable as it ensures that the ISMS is effective and compliant with relevant legislative, regulatory, contractual, and business requirements. As well, it ensures continual improvement to the organization's information security practices.</p>

This control is applicable as it ensures custodians or new staff have all the information they need for consistent and effective operations of systems to prevent the risk of critical failures and continue to operate critical services during the disruption.

This control is applicable as it manages the risk of compromising critical information of an organization and its customers and reduces the risks of poor performance related to hiring personnel that does not fulfill competence requirements.

This control is applicable as it ensures accountability of information security roles and responsibilities and it raises awareness amongst employees and contractors.

This control is applicable to keep employees and contractors up-to-date on the organization's information security policies and best practices to secure the organization's and its customers' information. Also, required to enhance the security knowledge and competence of employees continuously.

This control is applicable as it enforces information security policies and ensures that the organization can effectively respond to security breaches and employee negligence.

This control is applicable as it prevents unauthorized access or disclosure of the organization's confidential information. Additionally, the control ensures that important issues related to the termination process and internal role changes are addressed.

This control is applicable to ensure that the accountability of roles and responsibilities with respect to information security and confidentiality during information transfer.

<p>This control is applicable as the organization allows employees to work from home and therefore needs to protect the information accessed, processed, or stored at the remote working sites.</p>
<p>This control is applicable as it allows for the effective handling of information security events in a timely manner with respect to the confidentiality, integrity, and availability of the data of the organizations and its customers.</p>
<p>To protect areas containing sensitive or critical information from unauthorized physical access.</p>
<p>This control is applicable as it prevents unauthorized physical access to the organization's secure areas (such as data centers).</p>
<p>This control is applicable as it prevents unauthorized physical access to the organization's information processing facilities.</p>
<p>This control is applicable as it ensures that the organization's physical premises, critical access points, and information processing facilities are restricted to only authorized personnel.</p>
<p>This control is applicable as it protects against environmental threats that could impair the system's availability or information processing facilities.</p>
<p>This control is applicable to prevent unauthorized physical access to the organization's secure areas (such as data centers).</p>
<p>This control is applicable as it reduces the risks of unauthorized access, loss of, and damage to information assets during and outside normal working hours.</p>
<p>This control is applicable as it protects against environmental threats that could impair the system's availability or information processing facilities.</p>
<p>This control is applicable as it mitigates information disclosure risks and data loss when information assets are utilized outside the organization's premises.</p>
<p>This control is applicable to ensure only authorized disclosure, modification, removal, or destruction of information on storage media.</p>

This control is applicable as it protects against environmental threats that could impair the system's availability or information processing facilities.

This control is applicable as it ensures that infrastructure is protected from power failures and other disruptions that could cause unavailability of services and operations related to sabotage wiretapping and eavesdropping from the organization's office areas.

This control is applicable as it manages the risks of system failures and ensures devices are running efficiently and achieves continuous availability and integrity.

This control is applicable as it ensures equipment containing storage media (such as workstations hard-drives) with sensitive data is securely disposed of or overwritten so the data cannot be retrieved if the equipment is brought into the process for re-use.

Cloud Service Customer and Provider (ISO 27017): not applicable as the equipment is owned and managed by

~~See Trustworthy cloud service hosting providers~~
This control is applicable as it reduces risks related to unauthorized access on user endpoint devices, as information related to the organization and its customers is accessible through endpoint devices such as laptops and mobile phones.

This control is applicable as it manages the risks related to privileged access to networks and information systems.

This control is applicable as it minimizes the risks of unauthorized access to information assets owned by the organization as well as restricts access to customer data.

This control is applicable as it prevents unauthorized access to program source code which could impact the system's functionality and violate security requirements built-in within the development cycle

This control is applicable as it controls access to information systems in order to minimize the risk of unauthorized access to the organization and its customers' information.

This control is applicable as it ensures that the availability of information systems is in accordance with the organization's availability commitments.

This control is applicable to detect and protect information systems from malware and viruses. User awareness is critical to ensure users are aware of their roles and responsibilities for protecting systems from being infected by malware and virus attacks.

This control is applicable as it identifies potential technical vulnerabilities and develops an appropriate action plan in order to protect information systems against cybersecurity threats/breaches.

This control is applicable to ensure hardware, software, services, and networks function correctly with required security settings, and configurations are not altered by unauthorized or incorrect changes.

This control is applicable to prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

This control is applicable to limit the exposure of sensitive data (including PII) and to comply with legal, statutory, regulatory and contractual requirements.

This control is applicable to detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

This control is applicable to prevent the loss of data in the event of system failure and to ensure that data integrity and recoverability are retained if the data needs to be restored.

This control is applicable as it ensures that continuity of services provided by the organization to its customers.

This control is applicable to monitor activities within information systems in order to identify and analyze any issues in a timely manner while protecting logs from unauthorized access or tampering.

This control is applicable to ensure that events and activities within information systems are identified, monitored, and analyzed for issues.

This control is applicable as it ensures reliable operational log data and forensic data with timestamps from a trusted source.

Cloud Service Provider (ISO 27017): clock synchronization control is not applicable to OneTrust (as a cloud service provider).

This control is applicable as it manages risks related to unauthorized information disclosure through the use of a utility program.

Cloud Service Provider (ISO 27017): use of privileged utility program is not applicable to OneTrust (as a cloud service provider).

This control is applicable to reduce the risks of unauthorized changes/installations which could introduce security weaknesses within the information systems.

This control is applicable as it protects the data travels through the organization's network and other connected services from unauthorized access.

This control is applicable as it identifies the security mechanisms, service levels, and management requirements that need to be considered for securing network services.

This control is applicable as it protects the organization's network and the data that flows through it from the risk of unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.

This control is applicable to ensure that information systems are protected from malicious activities and attacks.

This control is applicable to define the controls and related procedures for various areas where encryption and other cryptographic techniques are employed within the organization.

This control is applicable as it is required to plan and manage a secure development effort for software and systems.

This control is applicable to secure and protect general, transactional, electronic order and payment information from risk of theft or data loss during data transmission.

This control is applicable to plan, control, and manage the design and implementation effort for information systems.

This control is applicable to ensure software is developed securely thereby reducing the number of potential information security vulnerabilities in the software.

This control is applicable to ensure that the system is functioning as expected and is in line with the organization's defined process for the software development lifecycle.

This control is applicable to ensure that the system is functioning as expected and inline with the organization's defined process for the software development lifecycle.

This control is applicable as it prevents unauthorized access or changes to the production environments and it ensures that changes are implemented as intended in the production environment.

This control is applicable in order to prevent unauthorized changes to information assets that affect the security and availability of systems while ensuring that changes are carried out in inline with the change management process.

This control is applicable in order to avoid the use of production data containing personal information or any other confidential information for test purposes. If production data is used, appropriate safeguards are required to protect the confidentiality of the data

This control is applicable to ensure that the ISMS of the organization continues to function effectively, meet the organization's commitments, and minimize the disruptions of business processes that may affect the organization and its customers

This control is applicable to ensure that signed third-party/vendor agreements include shared roles and responsibilities for information security in the use of the cloud services.

This control is applicable to ensure that signed third-party/vendor agreements include procedures to return and remove customers' assets in a timely manner upon the termination of the agreement.

This control is applicable to protect customers' virtual cloud environments from other customers and unauthorized access to customer data by segregating their computing environments.

This control is applicable to ensure that virtual machines in the cloud computing environments are configured to meet business needs using appropriate security and technical measures.

Cloud Service Provider (ISO 27017): erection of virtual machines is not applicable to the products/services of OneTrust (as a cloud service provider).

This control is applicable to ensure that there are procedures in place that define security and technical measures for administrative operations of a cloud computing environment.

This control is applicable to ensure that monitoring capabilities are enabled to monitor services in the cloud environments.

This control is applicable to ensure the consistency of configurations between virtual and physical networks as per the organization's network security policy.+G99:G103

Control Name
ISO 27701:2019 (PIMS)
PIMS - A.7.2.1 - Identify and document purpose
PIMS - A.7.2.2 - Identify lawful basis
PIMS - A.7.2.3 - Determine when and how consent is to be obtained
PIMS - A.7.2.4 - Obtain and Record Consent
PIMS - A.7.2.5 - Privacy Impact Assessment
PIMS - A.7.2.6 - Contracts with personal data processors
PIMS - A.7.2.7 - Joint Data Controller
PIMS - A.7.2.8 - Records related to processing personal data
PIMS - A.7.3.1 - Determining and fulfilling obligations to data subjects
PIMS - A.7.3.2 - Determining information for data subjects
PIMS - A.7.3.3 - Providing information to data subjects
PIMS - A.7.3.4 - Providing mechanism to modify or withdraw consent
PIMS - A.7.3.5 - Providing mechanism to object to personal data processing
PIMS - A.7.3.6 - Access, correction and/or erasure
PIMS - A.7.3.7 - Data controllers' obligations to inform third parties

PIMS - A.7.3.8 - Providing copy of personal data processed
PIMS - A.7.3.9 - Handling requests
PIMS - A.7.3.10 - Automated decision making
PIMS - A.7.4.1 - Limit collection
PIMS - A.7.4.2 - Limit processing
PIMS - A.7.4.3 - Accuracy and quality
PIMS - A.7.4.4 - Personal data minimization objectives
PIMS - A.7.4.5 - Personal data deidentification and deletion at the end of processing
PIMS - A.7.4.6 - Temporary files
PIMS - A.7.4.7 - Retention
PIMS - A.7.4.8 - Disposal
PIMS - A.7.4.9 - Personal Data Transmission Controls
PIMS - A.7.5.1 - Identify basis for personal data transfer between jurisdictions
PIMS - A.7.5.2 - Countries and international organizations to which personal data can be transferred.
PIMS - A.7.5.3 - Records of transfer of personal data
PIMS - A.7.5.4 - Records of personal data disclosure to third parties.

PIMS - B.8.2.1 - Customer agreement
PIMS - B.8.2.2 - Organization's purposes
PIMS - B.8.2.3 - Marketing and Advertising Use
PIMS - B.8.2.4 - Infringing Instruction
PIMS - B.8.2.5 - Customer Obligations
PIMS - B.8.2.6 - Records related to processing personal data
PIMS - B.8.3.1 - Obligations to data subjects
PIMS - B.8.4.1 - Temporary Files
PIMS - B.8.4.2 - Return, transfer or disposal of personal data
PIMS - B.8.4.3 - Personal data transmission controls
PIMS - B.8.5.1 - Basis for personal data transfer between jurisdictions
PIMS - B.8.5.2 - Countries and international organizations to which personal data can be transferred.
PIMS - B.8.5.3 - Records of personal data disclosure to third parties.
PIMS - B.8.5.4 - Notification of personal data disclosure requests.

PIMS - B.8.5.5 - Legally binding personal data disclosures.

PIMS - B.8.5.6 - Disclosure of subcontractors used to process personal data

PIMS - B.8.5.7 - Engagement of a subcontractor to process personal data

PIMS - B.8.5.8 - Change of subcontractor to process personal data

Control Description	Control Applicability	Implemented
The organization shall identify and document the specific purposes for which the personal data will be processed.	Yes	Yes
The organization shall determine, document and comply with the relevant lawful basis for the processing of personal data for the identified purposes.	Yes	Yes
The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of personal data was obtained from data subjects.	Yes	Yes
The organization shall obtain and record consent from data subjects according to the documented processes.	Yes	Yes
The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of personal data or changes to existing processing of personal data is planned.	Yes	Yes
The organization shall have a written contract with any data processor that it uses, and shall ensure that their contracts with data processors address the implementation of the appropriate controls	Yes	Yes
The organization shall determine respective roles and responsibilities for the processing of personal data (including personal data protection and security requirements) with any joint data controller.	No	Not Applicable
The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of personal data.	Yes	Yes
The organization shall determine and document their legal, regulatory and business obligations to data subjects related to the processing of their personal data and provide the means to meet these obligations.	Yes	Yes
The organization shall determine and document the information to be provided to data subjects regarding the processing of their personal data and the timing of such a provision.	Yes	Yes
The organization shall provide data subjects with clear and easily accessible information identifying the data controller and describing the processing of their personal data.	Yes	Yes
The organization shall provide a mechanism for data subjects to modify or withdraw their consent	Yes	Yes
The organization shall provide a mechanism for data subject to object to the processing of their personal data.	Yes	Yes
The organization shall implement policies, procedures and/or mechanisms to meet their obligations to data subjects to access, correct and/or erase their personal data.	Yes	Yes
The organization shall inform third parties with whom personal data has been shared of any modification, withdrawal or objections pertaining to the shared personal data, and implement appropriate policies, procedures and/or mechanisms to do so.	Yes	Yes

The organization shall be able to provide a copy of the personal data that is processed when requested by the data subject.	Yes	Yes
The organization shall define and document policies and procedures for handling and responding to legitimate requests from data subjects	Yes	Yes
The organization shall identify and address obligations, including legal obligations, to the data subjects resulting from decisions made by the organization which are related to the data subject based solely on automated processing of personal data.	Yes	Yes
The organization shall limit the collection of personal data to the minimum that is relevant, proportional and necessary for the identified purposes.	Yes	Yes
The organization shall limit the processing of personal data to that which is adequate, relevant and necessary for the identified purposes	Yes	Yes
The organization shall ensure and document that personal data is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the personal data	Yes	Yes
The organization shall ensure and document that personal data is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the personal data	Yes	Yes
The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.	Yes	Yes
The organization shall either delete personal data or render it in a form which does not permit identification or re-identification of data subjects, as soon as the original personal data is no longer necessary for the identified purpose(s).	Yes	Yes
The organization shall not retain personal data for longer than is necessary for the purposes for which the personal data is processed.	Yes	Yes
The organization shall have documented policies, procedures and/or mechanisms for the disposal of personal data	Yes	Yes
The organization shall subject personal data transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	Yes	Yes
The organization shall identify and document the relevant basis for transfers of personal data between jurisdictions.	Yes	Yes
The organization shall specify and document the countries and international organizations to which personal data can possibly be transferred.	Yes	Yes
The organization shall record transfers of personal data to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the data subjects.	Yes	Yes
The organization shall record disclosures of personal data to third parties, including what personal data has been disclosed, to whom and at what time.	Yes	Yes

The organization shall ensure, where relevant, that the contract to process personal data addresses the organization's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).	Yes	Yes
The organization shall ensure that personal data processed on behalf of a customer are only processed for the purposes expressed in the <u>documented instructions of the customer.</u>	Yes	Yes
The organization shall not use personal data processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate data subject. The organization shall not make providing such consent a condition for <u>receiving the service</u>	Yes	Yes
The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	Yes	Yes
The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with <u>their obligations.</u>	Yes	Yes
The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of personal data carried out on <u>behalf of a customer</u>	Yes	Yes
The organization shall provide the customer with the means to comply with its obligations related to data subjects.	Yes	Yes
The organization shall ensure that temporary files created as a result of the processing of personal data are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.	Yes	Yes
The organization shall provide the ability to return, transfer and/or disposal of personal data in a secure manner. It shall also make its policy <u>available to the customer</u>	Yes	Yes
The organization shall subject personal data transmitted over a data-transmission network to appropriate controls designed to ensure that the <u>data reaches its intended destination.</u>	Yes	Yes
The organization shall inform the customer in a timely manner of the basis for personal data transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to <u>such changes or to terminate the contract.</u>	Yes	Yes
The organization shall specify and document the countries and international organizations to which personal data can possibly be <u>transferred.</u>	Yes	Yes
The organization shall record disclosures of personal data to third parties, including what personal data has been disclosed, to whom and when	Yes	Yes
The organization shall notify the customer of any legally binding requests for disclosure of personal data.	Yes	Yes

The organization shall reject any requests for personal data disclosures that are not legally binding, consult the corresponding customer before making any personal data disclosures and accepting any contractually agreed requests for personal data disclosures that are authorized by the corresponding customer.	Yes	Yes
The organization shall disclose any use of subcontractors to process personal data to the customer before use.	Yes	Yes
The organization shall only engage a subcontractor to process personal data according to the customer contract.	Yes	Yes
The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process personal data, thereby giving the customer the opportunity to object to such changes.	Yes	Yes

This is applicable as adopted best practices and/or as results of risk assessment.
This is applicable as adopted best practices and/or as results of risk assessment.
This is applicable as adopted best practices and/or as results of risk assessment.
This is applicable as adopted best practices and/or as results of risk assessment.