Scope Statement	The certificate scope comprises the integrated management system (IMS) supporting the operations underlying the Thoropass platform offering. The organizational scope includes the Engineering and Operations teams affecting the management system.	ISO 4.3.0
Assets Included in Scope	Assets within the scope of the IMS include: customer data, software, people, and assets hosted on a cloud service provider (CSP). Thoropass abided by the shared security responsibility model provided by Amazon Web Services (AWS) in determining different responsibilities.	
Excluded from Scope	Employees primarily work remotely; however, Thoropass does maintain office space for employees to collaborate and work. Thoropass relies on data centers and physical hardware assets managed by a cloud service provider (CSP) under a service level agreement.	
Locations	Thoropass's mailing address is: 228 Park Ave. S., PMB 41082, New York, NY 10003	
Services	Thoropass develops and maintains a compliance software as a service platform to assist customers in achieving attestations, certifications, and other related security and privacy audits efficiently. Thoropass provides a hybrid approach of software with assigned subject matter expert professionals to assist the customer in their compliance journey. Thoropass may also perform specific audit and certification activities itself or through preferred audit partners leveraging Thoropass's integrated compliance platform.	
Context	Although Thoropass works in the compliance and regulatory standards industry, Thoropass is NOT considered part of the critical infrastructure.	ISO 4.1.0
Needs/Expectations	Thoropass's customers need and expect any information they provide to us to be kept secure and private. Thoropass is committed to security and privacy by abiding by federal, state, and local regulations such as the California Consumer Privacy Act (CCPA) as well as international privacy regulations such as the General Data Protection Regulation (GDPR) of the European Union (EU). Thoropass has certified to the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Thoropass also maintains contractual obligations through master service agreements, data protection agreements, and standard contractual clauses with customers. Security and privacy requirements are identified through the statement of applicability (SoA) of Thoropass's information security management system (ISMS) and privacy information management system (PIMS).	ISO 4.2.0
Results	Thoropass will establish, implement, maintain, and continually improve an IMS to include processes needed to satisfy ISO 27001 (security), ISO 27017 (cloud security), ISO 27701 (privacy), and ISO 27018 (cloud privacy) criteria.	ISO 4.4.0
Management's Commitment	Thoropass's management is committed to ensuring the following: a) information security and privacy policies and objectives are established as well as compatible with the strategic direction of Thoropass; b) information security management system (ISMS) and privacy information management system (PIMS) requirements are integrated into the organization's processes; c) ISMS and PIMS resources are available; d) information security and privacy management importance is communicated as well as conforms to the ISMS and PIMS requirements, respectively; e) ISMS and PIMS achieve intended outcomes; f) supporting persons and directions given contribute to the effectiveness of the ISMS and PIMS; g) continual improvement is promoted; and h) other relevant management roles are supported to demonstrate leadership applied to respective areas of responsibility.	ISO 5.1.0
	Thoropass's management will establish information security and privacy policies appropriate to Thoropass's purpose. The policies will include security and privacy objectives and follow a designated framework to set these information security and privacy objectives. Policies will establish a commitment to satisfy applicable information and privacy requirements as well as the continual improvement of the IMS. Policies will be documented, communicated, and made available to interested parties as appropriate.	ISO 5.2.0
	Thoropass's management assigned the Data Protection Officer (DPO)/Chief Information Security Officer (CISO) responsibility and authority to ensure the IMS conforms to documented requirement and performance of the IMS will be reported to top management.	ISO 5.3.0

27001 Security Annex A Controls	Control	Applicability	Justification	Status
05.01 Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Applicable	Thoropass maintains information security and privacy policies specifically defined, approved by management, published, communicated, and acknowledged by employees. Policies are reviewed at least annually or upon any significant changes.	Implemented
05.02 Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	Applicable	Thoropass formally assigns a Chief Information Security Officer and a Data Protection Officer responsible for security and privacy roles, respectively.	Implemented
05.03 Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	Applicable	Thoropass segregates conflicting duties and areas of responsibilities. For example, access approver and access administrator roles are assigned to different individuals along with audit/reviewer roles to reduce the risk of fraud, errors, and bypass information security and privacy safeguards.	Implemented
05.04 Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Applicable	Thoropass's management requires employees and contractors to apply information security and privacy according to established information security and privacy policies/processes.	Implemented
05.05 Contact with authorities	The organization should establish and maintain contact with relevant authorities.	Applicable	Thoropass establishes and maintains contact with authorities according to relevant regulatory or contractual obligations.	Implemented
05.06 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	Thoropass establishes and maintains contact with special interest groups and professional security as well as privacy associations such as HITRUST, Open Finance Data Security Standard (OFDSS), and the International Association of Privacy Professionals (IAPP), just to name a few.	Implemented
05.07 Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	Applicable	Thoropass stays up to date and informed on information security and privacy related threats. This information is collected, analyzed, and shared as part of threat intelligences to key stakeholders.	Implemented
05.08 Information security in project management	Information security should be integrated into project management.	Applicable	Thoropass integrates information security and privacy into project management activities.	Implemented
05.09 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Applicable	Thoropass develops and maintains an updated inventory of information/data as well as associated information assets to include owners.	Implemented
05.10 Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Applicable	Thoropass identifies, documents, and implements rules of acceptable use and behavior related to handling information and other associated assets.	Implemented
05.11 Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Applicable	Personnel or contractors assigned Thoropass owned assets must return these assets upon termination or change of employment or contract/agreement.	Implemented
05.12 Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Applicable	Thoropass classifies information according to security and privacy needs based on confidentiality, integrity, availability, and relevant requirements.	Implemented
05.13 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	Thoropass develops and implements a set of processes to label information according to Thoropass's Data Classification Scheme.	Implemented
05.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Applicable	Thoropass maintains transfer rules, processes, and agreements in place for all types of data transfers within Thoropass and between Thoropass and sub-processors/subcontractors.	Implemented
05.15 Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Applicable	Thoropass establishes and implements rules to control physical and logical access to information and information assets based on least privilege, minimum necessary, and role-based access per information security and privacy requirements.	Implemented
05.16 Identity management	The full life cycle of identities should be managed.	Applicable	Thoropass manages unique identifiers for each individual/user accessing information and information assets in order to assign appropriate access rights.	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
05.17 Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Applicable	Thoropass allocates and manages authentication information through a formal management process to include making employees and contractors aware of appropriate handling of authentication information.	Implemented
05.18 Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Applicable	Thoropass provisions, reviews, modifies, and removes access rights to information and assets according to Thoropass's Access Control Policy and access control rules based on business requirements.	Implemented
05.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Applicable	Thoropass defines and implements process to manage security and privacy risks with the use of supplier's/vendor's products/services. Thoropass performs security, privacy, and trade sanction reviews of vendors/contractors as well as ensure agreements containing security and privacy requirements are in place with vendors/contractors.	Implemented
05.20 Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Applicable	Thoropass establishes agreed upon security and privacy requirements for each supplier/vendor/contractor based on the type of relationship. Thoropass performs security, privacy, and trade sanction reviews of vendors/contractors.	Implemented
05.21 Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Applicable	Thoropass defines and implements processes to manage security and privacy risks associated with information and communication technology (ICT) products/services. Thoropass performs security, privacy, and trade sanction reviews of vendors/contractors as well as ensure agreements containing security and privacy requirements are in place with vendors/contractors.	Implemented
05.22 Monitoring, review and change management of supplier services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Applicable	Thoropass regularly monitors, reviews, and evaluates as well as manage any changes with supplier/vendor/contractor information security and privacy practices along with service delivery in line with agreements.	Implemented
05.23 Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	Applicable	Thoropass establishes processes for acquiring, using, managing, and exiting cloud services according to information security and privacy requirements.	Implemented
05.24 Information security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Applicable	Thoropass plans and prepares for information security and privacy incidents by defining, establishing, and communicating security/privacy incident management processes, roles, and responsibilities.	Implemented
05.25 Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	Applicable	Thoropass assesses all information security and privacy events to determine if they need to be categorized as an information security and/or privacy incident.	Implemented
05.26 Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Applicable	Thoropass responds to information security and privacy incidents according to documented processes.	Implemented
05.27 Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Applicable	Thoropass performs an after action review of all security and privacy incidents to gain further knowledge in order to strengthen and improve the information security/privacy controls as well as reduce the likelihood/consequences of future incidents.	Implemented
05.28 Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Applicable	Thoropass establishes and implements processes to identify, collect, acquire, and preserve evidence for the purposes of disciplinary/legal actions related to information security/privacy events. Thoropass evaluates and vets digital forensic experts.	Implemented
05.29 Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Applicable	Thoropass maintains plans to protect information and other assets during a disruption.	Implemented
05.30 ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Applicable	Thoropass plans, implements, maintains, and tests information and communication technology (ICT) readiness based on Thoropass's business continuity objectives and ICT continuity requirements during a disruption.	Implemented
05.31 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 should be identified, documented and kept up to date.	Applicable	Thoropass identifies, documents, and is kept up to date on Thoropass's approach to meet the legal, statutory, regulatory, and contractual requirements relevant to information security and privacy.	Implemented
05.32 Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	Applicable	Thoropass implements appropriate processes to protect intellectual property rights and use of proprietary products in compliance with legal, statutory, regulatory, and contractual requirements. Thoropass requires all employees and contractors to sign a non-disclosure agreement.	Implemented
05.33 Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Applicable	Thoropass implements safeguards to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release.	Implemented
05.34 Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Applicable	Thoropass identifies and meets requirements related to information security and the preservation of privacy regarding the protection of personally identifiable information (PII) according to applicable regulations and contractual obligations.	Implemented
05.35 Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Applicable	Thoropass performs independent reviews to management's approach and implementation of information security and privacy to include people, processes, and technologies at planned intervals (i.e. annually), or when significant changes occur, to ensure continuing suitability, adequacy, and effectiveness.	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
05.36 Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Applicable	Thoropass performs regular reviews of compliance with information security and privacy policies, processes, rules, and standards.	Implemented
05.37 Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Applicable	Thoropass documents and makes available to appropriate personnel operating procedures for information processing facilities to ensure correct and secure operations.	Implemented
06.01 Screening	Background verification checks on all candidates to become personnel should 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.	Applicable	Thoropass performs background verification checks on all candidates prior to employment and on an ongoing basis considering applicable regulations, ethics, and risks to business operations.	Implemented
06.02 Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Applicable	Employees are made aware of their responsibility for information security and privacy through defined job requirements, employee agreements, and training.	Implemented
06.03 Information security awareness, education and training	Personnel of the organization and relevant interested parties should 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	Thoropass's employees receive appropriate information security and privacy awareness, education, and training upon hire and annually thereafter to include information security and privacy policies/procedures as well as relevant job functions.	Implemented
06.04 Disciplinary process	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Applicable	Thoropass maintains a formal disciplinary process communicated to employees who have committed an information security and/or privacy policy violation. The disciplinary process is intended to make employees aware of consequences of violations, to deter violations from happening, and appropriately deal with employees who have committed a violation.	Implemented
06.05 Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Applicable	Thoropass defines, enforces, and communicates to employees their information security and privacy responsibilities/duties remaining valid after termination or change of employment.	Implemented
06.06 Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Applicable	Thoropass identifies, documents, regularly reviews, and requires employees to sign confidentiality (or non-disclosure) agreements reflecting Thoropass's needs for the protection of information to maintain confidentiality of information accessible by the employee.	Implemented
06.07 Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Applicable	Thoropass implements security and privacy measures for employees working remotely to protect information access, processed, or stored outside of Thoropass's premises.	Implemented
06.08 Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Applicable	Thoropass provides mechanisms for employees to report observed (or suspected) information security and/or privacy events through their managers or directly to the CISO/DPO in a timely manner.	Implemented
07.01 Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including physical security perimeters. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.02 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including physical entry. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.03 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including securing offices, rooms and facilities. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.04 Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including physical security monitoring. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.05 Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including protection against physical and environmental threats. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.06 Working in secure areas	Security measures for working in secure areas should be designed and implemented.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including working in secure areas. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
07.07 Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Applicable	Thoropass defines and appropriately enforces clear desk rules for paper and clear screen rules for information processing facilities to reduce risks of unauthorized access and loss/damage to information during/outside of normal working hours.	Implemented
07.08 Equipment siting and protection	Equipment should be sited securely and protected.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including equipment sitting and protection. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.09 Security of assets off-premises	Off-site assets should be protected.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including security of assets off-premises. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.10 Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including storage media. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.11 Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including supporting utilities. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.12 Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including cabling security. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.13 Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including equipment maintenance. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
07.14 Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Applicable	Thoropass leverages a third-party, Amazon Web Services (AWS), as its IaaS provider. AWS maintains responsibility for physical security over its data centers, including secure disposal or re-use of equipment. Thoropass validates these controls as part of its third-party due dilligence efforts	Implemented
08.01 User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Applicable	Thoropass protects information stored on, process by, or accessible via user endpoint devices.	Implemented
08.02 Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	Applicable	Thoropass restricts and manages the allocation as well as use of privileged access rights to ensure only authorized users, software components, and services are provided with appropriate privileged access rights.	Implemented
08.03 Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Applicable	Thoropass restricts access to information and other associated assets according to Thoropass's Access Control Policy to ensure only authorized access (and to prevent unauthorized access) to information and other assets.	Implemented
08.04 Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	Applicable	Thoropass appropriately manages read/write access to source code, development tools, and software libraries to prevent the introduction of unauthorized functionality, avoid unintentional/malicious changes, and to maintain the confidentiality of valuable intellectual property.	Implemented
08.05 Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Applicable	Thoropass implements secure authentication technologies and processes based on information access restricted according to Thoropass's Access Control Policy to ensure a user (or an entity) is securely authentication when accessing approved systems, applications, and services.	Implemented
08.06 Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Applicable	Thoropass monitors and adjusts the use of resources in line with current and expected capacity requirements to ensure the required capacity of information processing facilities, human resources, offices, and other facilities.	Implemented
08.07 Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	Applicable	Thoropass implements and supports through appropriate user awareness the protection against malware.	Implemented
08.08 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Applicable	Thoropass obtains information about technical vulnerabilities of information systems in use. Thoropass evaluates exposures to such vulnerabilities and takes appropriate measures to prevent exploitation of technical vulnerabilities.	Implemented
08.09 Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Applicable	Thoropass establishes, documents, implements, monitors, and reviews configurations (including security configurations) of hardware, software, services, and networks to ensure correct functions with required security settings as well as ensure configurations are not altered by unauthorized (or incorrect) changes.	Implemented
08.10 Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Applicable	Thoropass deletes information stored in information systems, devices, or in any other storage media when no longer required to prevent unnecessary exposure of sensitive information as well as comply with regulatory and contractual obligations for information deletion.	Implemented
08.11 Data masking	Data masking should 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.	Not Applicable	Not Applicable. Thoropass does not perform any data masking as part of its service offering and data masking protection doesn't apply to the type of data collected through Thoropass's platform.	Not Applicable
08.12 Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Applicable	Thoropass has implemented a mobile device management solution, SIEM, and a content-filtering solution to assist in data loss prevent (DLP) applied to systems, networks, and any other devices that process, store, or transmit sensitive information.	Implemented
08.13 Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Applicable	Thoropass maintains a synchronized copy of customer data. Thoropass utilizes web-based applications and back-up copies of system images as necessary. Backup routines are regularly tested according to Thoropass's Contingency Plan Policy and processes.	Implemented
08.14 Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Applicable	Thoropass implements redundancy processes at the facility to meet availability requirements. Thoropass utilizes a remote work staff and leverages the redundancies of a Cloud Service Provider (i.e. AWS).	Implemented
08.15 Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Applicable	Thoropass produces, stores, protects, and analyzes logs recording activities, exceptions, faults, and other relevant events. Thoropass record events, generate evidence, ensure integrity of logs, prevent unauthorized access to logs, and identify information security or privacy events leading to an incident as well as support investigations.	Implemented
08.16 Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Applicable	Thoropass monitors networks, systems, and applications for anomalous behavior and takes appropriate actions to evaluate potential information security and privacy incidents.	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
08.17 Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Applicable	Thoropass ensures clocks of information processing systems used are synchronized to approved time sources to enable the correlation/analysis of security- or privacy-related events and other recorded data. Thoropass utilizes time synchronization to support investigations into information security and privacy incidents.	Implemented
08.18 Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Applicable	Thoropass restricts and tightly control the use of utility programs capable of overriding system or application controls to ensure the utility programs do not harm system/application controls for information security or privacy.	Implemented
08.19 Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Applicable	Thoropass implements processes and safeguards to securely manage software installation on operational systems to ensure the integrity of operational systems as well as prevent exploitation of technical vulnerabilities.	Implemented
08.20 Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Applicable	Thoropass secures, manages, and controls networks and network devices to protect information in systems/applications. Thoropass utilizes AWS to ensure physical protection over network devices and leverages native AWS tools within a virtual private cloud (VPC) to protect Thoropass's platform.	Implemented
08.21 Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Applicable	Thoropass identifies, implements, and monitors security mechanisms, service levels, and service requirements of network services. Thoropass identifies, implements, and monitors security mechanisms, service levels, and service requirements of AWS services hosting the Thoropass Platform.	Implemented
08.22 Segregation of networks	Groups of information services, users and information systems should be segregated in the organization’s networks.	Applicable	Thoropass segregates production, testing, and development environments for the Thoropass Platform.	Implemented
08.23 Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Applicable	Thoropass implements a content and web-filtering solution to manage and reduce exposure to malicious content via accessing external websites	Implemented
08.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Applicable	Thoropass defines and implements rules for the effective use of cryptography including cryptographic key management to protect the confidentiality, authenticity, or integrity of information according to business, security, and privacy requirements as well as taking into consideration regulatory and contractual requirements related to cryptography.	Implemented
08.25 Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	Applicable	Thoropass establishes and applies rules for the secure development of software and systems to ensure information security and privacy is designed as well as implemented within the secure development life cycle of software/systems.	Implemented
08.26 Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Applicable	Thoropass identifies, specifies, and approves information security and privacy related requirements when developing (or acquiring) applications.	Implemented
08.27 Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Applicable	Thoropass establishes, documents, maintains, and applies principles of engineering secure systems to any information system development activities.	Implemented
08.28 Secure coding	Secure coding principles should be applied to software development.	Applicable	Thoropass applies secure coding principles to software development to ensure software is written security to reduce the number of potential information security vulnerabilities in the software.	Implemented
08.29 Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	Applicable	Thoropass defines and implements security testing process in the development life cycle to validate information security and privacy requirements are met when applications (or code) are deployed to the production environment.	Implemented
08.30 Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	Applicable	Thoropass directs, monitors, and reviews the activities related to outsourced system development to ensure information security and privacy measures are implemented.	Implemented
08.31 Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	Applicable	Thoropass separates and secures the development, testing, and production environments and data from compromise by development/test activities.	Implemented
08.32 Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Applicable	Thoropass subjects changes to the information processing facilities and information systems to the change management process. Thoropass implements its change management process when making changes to the Thoropass Platform to preserve information security and privacy when executing changes.	Implemented
08.33 Test information	Test information should be appropriately selected, protected and managed.	Applicable	Thoropass appropriately selects, protects, and manages test information to ensure relevance of testing along with protection of operational information used for testing.	Implemented
08.34 Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Applicable	Thoropass plans and agreements are made between testers and appropriate management when audit tests (and other assurance activities) involve the assessment of operational systems in order to minimize the impact of audit activities on business processes.	Implemented
ISO 27017 - CCSP Security Extended Control Set	**Control**	**Applicability**	**Justification**	**Status**
CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment	CLD.6.3 Relationship between cloud service customer and cloud service provider Objective: To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management. Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.	Applicable	Thoropass defines or extends its existing policies and procedures in accordance with its use of cloud services, and make cloud service users aware of their roles and responsibilities in the use of the cloud service. Thoropass, as a cloud service provider, documents and communicates its information security capabilities, roles, and responsibilities for the use of its cloud service, along with the information security roles and responsibilities for which customers would need to implement and manage as part of its use of the cloud services offered by Thoropass. This is documented and communicated through terms of service, master service agreements, or other related agreements.	Implemented
CLD.8.1.5 Removal of cloud service customer assets	CLD.8.1 Responsibility for assets - The objective specified in clause 8.1 of ISO/IEC 27002 applies. Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	Applicable	Thoropass requests a documented description of the termination of service process covering the return and removal of Thoropass's assets followed by the deletion of all copies of those assets from the cloud service provider's systems. The description lists all the assets and document the schedule for the termination of service, which should occur in a timely manner. Thoropass, as a cloud service provider, provides information about the arrangements for the return and removal of any customer’s assets upon termination of the agreement for the use of a cloud service. The asset return and removal arrangements are documented in the agreement and are performed in a timely manner. The arrangements specify the assets to be returned and removed.	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
CLD.9.5.1 Segregation in virtual computing environments	CLD.9.5 Access control of cloud service customer data in shared virtual environment Objective: To mitigate information security risks when using the shared virtual environment of cloud computing A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.	Applicable	Thoropass, as a cloud service provider, enforces appropriate logical segregation of customer data, virtualized applications, operating systems, storage, and network for: the separation of resources used by customers in multi-tenant environments; and the separation of Thoropass's internal administration from resources used by customers. Where the cloud service involves multi-tenancy, Thoropass implements information security controls to ensure appropriate isolation of resources used by different tenants (i.e., customers). Thoropass considers the risks associated with running customer-supplied software within the cloud services offered by Thoropass.	Implemented
CLD.9.5.2 Virtual machine hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.	Applicable	When configuring virtual machines, Thoropass (as a cloud customer) and cloud service providers as well as Thoropass (as a cloud service provider) and Thoropass's customers ensure appropriate aspects are hardened (e.g., only those ports, protocols, and services required), and the appropriate technical measures are in place (e.g., anti-malware and logging) for each virtual machine used.	Implemented
CLD.12.1.5 Administrator's operational security	CLD.12.1 Operational procedures and responsibilities - The objective specified in clause 12.1 of ISO/IEC 27002 applies. Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.	Applicable	Thoropass documents procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment. The document specifies a supervisor will monitor these operations. Thoropass, as a cloud service provider, provides documentation about the critical operations and procedures to customers who require it.	Implemented
CLD.12.4.5 Monitoring of Cloud Services	CLD.12.4 Logging and monitoring - The objective specified in clause 12.4 of ISO/IEC 27002 applies. The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	Applicable	Thoropass requests information from the cloud service provider of the service monitoring capabilities available for each cloud service. Thoropass, as a cloud service provider, provides capabilities enabling customers to monitor specific aspects, relevant to the customer, of the operation of the cloud services. Appropriate access controls secure the use of the monitoring capabilities. The capabilities provide access only to information about the customer's own cloud service instances. Thoropass provides documentation of the service monitoring capabilities to customers. Monitoring provides data consistent with the event logs and assist with service level agreement (SLA) terms.	Implemented
CLD.13.1.4 Alignment of security management for virtual and physical networks	CLD.13.1 Network security management The objective specified in clause 13.1 of ISO/IEC 27002 applies. Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.	Applicable	Thoropass, as a cloud service provider, defines and documents an information security policy for the configuration of the virtual network consistent with the information security policy for a physical network, if applicable. Thoropass ensures the virtual network configuration matches the information security policy regardless of the means used to create the configuration.	Implemented
ISO 27701 Privacy	**Control**	**Applicability**	**Justification**	**Status**
07.02.01 Identify and document purpose	The organization should identify and document the specific purposes for which the PII will be processed.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.02.02 Identify lawful basis	The organization should determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.02.03 Determine when and how consent is to be obtained	The organization should determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.02.04 Obtain and record consent	The organization should obtain and record consent from PII principals according to the documented processes.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.02.05 Privacy impact assessment	The organization should assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.02.06 Contracts with PII processors	The organization should have a written contract with any PII processor that it uses, and should ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex B.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.02.07 Joint PII controller	The organization should determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.02.08 Records related to processing PII	The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.01 Determining and fulfilling obligations to PII principals	The organization should determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.02 Determining information for PII principals	The organization should determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.03 Providing information to PII principals	The organization should provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.04 Providing mechanisms to modify or withdraw consent	The organization should provide a mechanism for PII principals to modify or withdraw their consent.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.05 Providing mechanism to object to PII processing	The organization should provide a mechanism for PII principals to object to the processing of their PII.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.06 Access, correction and/or erasure	The organization should implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.07 PII controllers' obligations to inform third parties	The organization should inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures and/or mechanisms to do so.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.08 Providing copy of PII processed	The organization should be able to provide a copy of the PII that is processed when requested by the PII principal.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.09 Handling requests	The organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.03.10 Automated decision making	The organization should identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable

27001 Security Annex A Controls	Control	Applicability	Justification	Status
07.04.01 Limit collection	The organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.02 Limit processing	The organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.03 Accuracy and quality	The organization should ensure and document that PII 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 PII.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.04 PII minimization objectives	The organization should define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.05 PII de-identification and deletion at the end of processing	The organization should either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.06 Temporary files	The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.07 Retention	The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.08 Disposal	The organization should have documented policies, procedures and/or mechanisms for the disposal of PII.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.04.09 PII transmission controls	The organization should subject PII 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.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.05.01 Identify basis for PII transfer between jurisdictions	The organization should identify and document the relevant basis for transfers of PII between jurisdictions.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.05.02 Countries and international organizations to which PII can be transferred	The organization should specify and document the countries and international organizations to which PII can possibly be transferred.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.05.03 Records of transfer of PII	The organization should record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
07.05.04 Records of PII disclosure to third parties	The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.	Not Applicable	Not Applicable. Thoropass is a processor and NOT a controller.	Not Applicable
08.02.01 Customer agreement	The organization should ensure, where relevant, that the contract to process PII 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).	Applicable	Thoropass ensures contracts to process PII address Thoropass's role in providing assistance with the customer's obligations (taking into account nature of processing and information available to Thoropass).	Implemented
08.02.02 Organization's purposes	The organization should ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.	Applicable	Thoropass only processes PII on behalf of a customer for the pruposes expressed in the documented instructions of the customer.	Implemented
08.02.03 Marketing and advertising use	The organization should not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization should not make providing such consent a condition for receiving the service.	Applicable	Thoropass does not use PII processed under a contract for the purposes of marketing or advertising without prior consent obtained from the appropriate PII principal. Thoropass does not make providing such consent as a condition for receiving Thoropass's services or products.	Implemented
08.02.04 Infringing instruction	The organization should inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.	Applicable	Thoropass will inform a customer if a processing instruction infringes applicable legislation and/or regulation.	Implemented
08.02.05 Customer obligations	The organization should provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.	Applicable	Thoropass provides customers with any appropriate information so the customer can demonstrate compliance with any of their obligations regarding PII.	Implemented
08.02.06 Records related to processing PII	The organization should determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.	Applicable	Thoropass determines and maintains necessary records to support demonstrating compliance with obligations as may be specific in applicable contracts for the processing of PII carried out on behalf of a customer. Thoropass has completed a GDPR and CCPA self-assessment available through Thoropass's Trust Center. Thoropass is also certified to the EU-US DPF certification.	Implemented
08.03.01 Obligations to PII principals	The organization should provide the customer with the means to comply with its obligations related to PII principals.	Applicable	Thoropass provides customers with the means to comply with its obligations related to PII principals.	Implemented
08.04.01 Temporary Files	The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.	Applicable	Thoropass ensures temporary files created as a result of processing of PII are disposed of according to Thoropass's data destruction policies/procedures within specific time periods outlined in Thoropass's data retention schedule.	Implemented
08.04.02 Return, transfer, or disposal of PII	The organization should provide the ability to return, transfer and/or disposal of PII in a secure manner. It should also make its policy available to the customer.	Applicable	Thoropass provides for the ability to return, transfer, and/or dispose of PII in a secure manner. Thoropass makes privacy notices, data protection agreements, standard contractual clauses, and attestations/certifications regarding security and privacy available to customers.	Implemented
08.04.03 PII transmission controls	The organization should subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.	Applicable	Thoropass encrypts all sensitive information and PII over a data-transmission network utilizing at least TLSv1.2 or later designed to ensure data reaches its intended desitation securely.	Implemented
08.05.01 Basis for PII transfer between jurisdictions	The organization should inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.	Applicable	Thoropass abides by the EU-US DPF and informs customers in a timely manner of any basis for PII transfers between jurisdictions and of any intended changes in transfers.	Implemented
08.05.02 Countries and international organizations to which PII can be transferred	The organization should specify and document the countries and international organizations to which PII can possibly be transferred.	Applicable	Thoropass specifies and documents the US as the country that stores and processes PII. Thoropass does not transfer PII to any other country.	Implemented
08.05.03 Records of PII disclosure to third parties	The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.	Applicable	Thoropass will maintain records of disclosures of PII to third parties, including what PII has been disclosed, to whom, and when. Thoropass maintains a list of approved subprocessors containing this information and all controllers are notified of this disclosure (or any changes to the subprocessor list).	Implemented
08.05.04 Notification of PII disclosure requests	The organization should notify the customer of any legally binding requests for disclosure of PII.	Applicable	Thoropass will notify the customer of any legally binding requests for disclosure of PII within its privacy notice and contracts.	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
08.05.05 Legally binding PII disclosures	The organization should reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.	Applicable	Thoropass will reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures, and accept any contractually agreed requests for PII discloosures authorized by the corresponding customer. Thoropass makes this known with its privacy notice, data protection addendum, standard contractual clauses, and certification to the EU-US DPF to the customer.	Implemented
08.05.06 Disclosure of subcontractors used to process PII	The organization should disclose any use of subcontractors to process PII to the customer before use.	Applicable	Thoropass notifies and obtains approval from customers for any disclosure of any use of subcontractors to process PII to the customer before use.	Implemented
08.05.07 Engagement of a subcontractor to process PII	The organization should only engage a subcontractor to process PII according to the customer contract.	Applicable	Thoropass only engages subcontractors to process PII according to the customer contract.	Implemented
08.05.08 Change of subcontractor to process PII	The organization should, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.	Applicable	Thoropass informs the customer of any intended changes concerning the addition/replacement of subcontractors to process PII, therby giving the customer the opportunity to object to such changes. A list of subcontractors are maintained within Thoropass's Trust Center. Notification is sent to controllers/customers when this list of subcontractors changes.	Implemented
ISO 27018 - CCSP Privacy Extended Control Set	**Control**	**Applicability**	**Justification**	**Status**
A.1 General				
A.2.1 Obligation to co-operate regarding PII principals' rights	A.2 Consent and choice A.2.1 Obligation to co-operate regarding PII principals' rights Control The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.	Applicable	Where the PII controller depends on Thoropass for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures are specified in the contract.	Implemented
A.3.1 Public cloud PII processor's purpose	A.3 Purpose legitimacy and specification A.3.1 Public cloud PII processor's purpose Control PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.	Applicable	Thoropass providea the customer with all relevant information, in a timely fashion, to allow the customer to ensure Thoropass's compliance with purpose specification and limitation principles and ensure no PII is processed by Thoropass (or any of its subcontractors) for further purposes independent of the instructions of the customer.	Implemented
A.3.2 Public cloud PII processor's commercial use	A.3.2 Public cloud PII processor's commercial use Control PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service. NOTE This control is an addition to the more general control in A.3.1 and does not replace or otherwise supersede it.	Applicable	PII processed under a contract is not be used by Thoropass for the purposes of marketing and advertising without express consent. Such consent will not be a condition of receiving the service.	Implemented
A.4 Collection limitation	No additional controls are relevant to this privacy principle.	Applicable	No additional controls are relevant to this privacy principle. Thoropass limits the collection of PII to what is necessary to provide the services under contract to a customer.	Implemented
A.5.1 Secure erasure of temporary files	A.5 Data minimization A.5.1 Secure erasure of temporary files Control Temporary files and documents should be erased or destroyed within a specified, documented period.	Applicable	PII processing information systems implement a periodic check that unused temporary files above a specified age are deleted.	Implemented
A.6.1 PII disclosure notification	A.6 Use, retention and disclosure limitation A.6.1 PII disclosure notification Control The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	Applicable	Thoropass provides contractual guarantees to: reject any requests for PII disclosure that are not legally binding; consult the corresponding customer where legally permissible before making any PII disclosure; and accept any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.	Implemented
A.6.2 Recording of PII disclosures	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.	Applicable	PII may be disclosed during the course of normal operations. These disclosures are recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, are also recorded. The records include the source of the disclosure and the source of the authority to make the disclosure.	Implemented
A.7 Accuracy and quality	No additional controls are relevant to this privacy principle.	Applicable	No additional controls are relevant to this privacy principle. Thoropass maintains the accuracy and quality of PII provided by customers by providing customers the ability to ensure accuracy of the PII information they provide or by making the appropriate corrections instructed by a customer to ensure quality of PII information.	Implemented
A.8.1 Disclosure of sub-contracted PII processing	A.8 Openness, transparency and notice A.8.1 Disclosure of sub-contracted PII processing Control The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.	Applicable	Provisions for the use of subcontractors to process PII are transparent in the contract between Thoropass and the customer. The contract specifies subcontractors can only be commissioned on the basis of a consent generally being given by the customer at the beginning of the service. Thoropass informs the customer in a timely fashion of any intended changes in this regard so the customer has the ability to object to such changes or to terminate the contract. Information disclosed covers the fact subcontracting is used and the names of relevant subcontractors, but not any business-specific details. The information disclosed also includes the countries in which subcontractors can process data (see A.12.1) and the means by which subcontractors are obliged to meet (or exceed) the obligations of Thoropass (see A.11.12). Where public disclosure of subcontractor information is assessed to increase security risk beyond acceptable limits, disclosure is made under a non-disclosure agreement and/or on the request of the customer. The customer is made aware the information is available.	Implemented
A.9 Individual participation and access	No additional controls are relevant to this privacy principle.	Applicable	No additional controls are relevant to this privacy principle. Thoropass, as a processor, directs individuals to obtain requests for access from a customer (i.e., controller). The customer directs Thoropass, as needed, to provide access to PII information of an individual. Customers, as controllers, must obtain necessary consent from an individual for Thoropass to process their PII on behalf of a customer under contract.	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
A.10.1 Notification of a data breach involving PII	A.10 Accountability A.10.1 Notification of a data breach involving PII Control The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.	Applicable	Thoropass promptly notifies the customer in the event of any unauthorized access to PII or unauthorized access to processing equipment (or facilities) resulting in loss, disclosure, or alteration of PII. Provisions covering the notification of a data breach involving PII form part of the contract between Thoropass and the customer. The contract specifies how Thoropass will provide the information necessary for the customer to fulfill their obligation to notify relevant authorities. This notification obligation does not extend to a data breach caused by the customer (or PII principal) or within system components for which they are responsible. The contract also define the maximum delay in notification of a data breach involving PII. In the event a data breach involving PII has occurred, a record will be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident (including the person in charge and the data recovered), and the fact the incident resulted in loss, disclosure, or alteration of PII. In the event a data breach involving PII has occurred, the record also includes a description of the data compromised, if known; and if notifications were performed, the steps taken to notify customers (and/or regulatory agencies).	Implemented
A.10.2 Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures should be retained for a specified, documented period on replacement (including updating).	Applicable	Review of current and historical policies and procedures may be required such as in the cases of customer dispute resolution and investigation by a PII protection authority. Thoropass maintains and retains policies and procedures for six (6) years from date of creation or date when last in effect, whichever is later, according to the Data Retention Schedule.	Implemented
A.10.3 PII return, transfer and disposal	The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.	Applicable	Thoropass maintains a policy regarding the return, transfer, and/or disposal of PII and makes this policy available to the customer. Thoropass provides the information necessary to allow the customer to ensure PII processed under a contract is erased (by Thoropass and any of its subcontractors) from wherever they are stored (including for the purposes of backup and business continuity) as soon as they are no longer necessary for the specific purposes of the customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards is provided for contractually. Thoropass develops and implements a policy in respect of the disposition of PII and makes this policy available to customers. The policy covers the retention period for PII before its destruction after termination of a contract, to protect the customer from losing PII through an accidental lapse of the contract.	Implemented
A.11.1 Confidentiality or non-disclosure agreements	A.11 Information security A.11.1 Confidentiality or non-disclosure agreements Control Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	Applicable	Individuals under Thoropass's control with access to PII are subject to a confidentiality obligation. A confidentiality agreement, in whatever form, between Thoropass, its employees, and its agents ensures employees (and agents) do not disclose PII for purposes independent of the instructions of the customer (see A.3.1). The obligations of the confidentiality agreement survives termination of any relevant contract.	Implemented
A.11.2 Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted.	Applicable	The creation of hardcopy material displaying PII is restricted.	Implemented
A.11.3 Control and logging of data restoration	There should be a procedure for, and a log of, data restoration efforts.	Applicable	Thoropass maintains a procedure for (and a log of) data restoration efforts. The log of data restoration efforts contains: the person responsible, a description of the restored data, and the data that were restored manually.	Implemented
A.11.4 Protecting data on storage media leaving the premises	PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	Applicable	PII on media leaving Thoropass's premises is subject to an authorization procedure and is not accessible to anyone other than authorized personnel (such as by encrypting the data concerned).	Implemented
A.11.5 Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	Applicable	Portable physical media and portable devices that do not permit encryption is not to be used (except where it is unavoidable and any use of such portable media/devices is documented).	Implemented
A.11.6 Encryption of PII transmitted over public data-transmission networks	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.	Applicable	PII transmitted over public data-transmission networks is encrypted prior to transmission.	Implemented
A.11.7 Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Applicable	Where hardcopy materials are destroyed, they are destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Implemented
A.11.8 Unique use of user IDs	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	Applicable	If more than one individual has access to stored PII, then they each have a distinct user ID for identification, authentication, and authorization purposes.	Implemented
A.11.9 Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.	Applicable	An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained. A user profile is maintained for all users whose access is authorized by Thoropass. The profile of a user comprises the set of data about that user (including user ID) necessary to implement the technical controls providing authorized access to the information system.	Implemented
A.11.10 User ID management	De-activated or expired user IDs should not be granted to other individuals.	Applicable	Deactivated (or expired) user IDs are not granted to other individuals.	Implemented
A.11.11 Contract measures	Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.	Applicable	Contracts between the customer and Thoropass specify minimum technical and organizational measures to ensure the contracted security arrangements are in place and data are not processed for any purpose independent of the instructions of the controller. Such measures are subject to unilateral reduction by Thoropass. Information security and PII protection obligations relevant to Thoropass may arise directly from applicable law. Where this is not the case, PII protection obligations relevant to Thoropass are covered in the contract. Thoropass informs a prospective customer, before entering into a contract, about the aspects of its services material to the protection of PII. Thoropass is transparent about its capabilities during the process of entering into a contract; however, it is ultimately the customer's responsibility to ensure the measures implemented by Thoropass meet its obligations.	Implemented

27001 Security Annex A Controls	Control	Applicability	Justification	Status
A.11.12 Sub-contracted PII processing	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.	Applicable	Contracts between Thoropass and any subcontractors processing PII specify minimum technical and organizational measures meeting the information security and PII protection obligations of Thoropass. Such measures are not subject to unilateral reduction by the subcontractor.	Implemented
A.11.13 Access to data on pre-used data storage space	The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.	Applicable	Thoropass ensures whenever data storage space is assigned to a customer, any data previously residing on that storage space is not visible to that customer.	Implemented
A.12.1 Geographical location of PII	A.12 Privacy compliance A.12.1 Geographical location of PII Control The public cloud PII processor should specify and document the countries in which PII can possibly be stored.	Applicable	Thoropass specifies and documents the countries in which PII can possibly be stored. The identities of the countries where PII can possibly be stored (i.e., US) is made available to customers. The identities of the countries arising from the use of subcontracted PII processing is included. Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the agreements and the countries (or circumstances in which such agreements apply) is also identified. Thoropass informs the customer in a timely fashion of any intended changes in this regard so the customer has the ability to object to such changes or to terminate the contract.	Implemented
A.12.2 Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	Applicable	PII transmitted using a data-transmission network is subject to appropriate controls designed to ensure data reaches its intended destination.	Implemented