SOA - STATEMENT OF APPLICABILITY REV 01 14.12.2023						
ISO/IEC 27001:2022						
Categoria	Codice	Titolo ita	Controllo	Estensione ISO 27017	Estensione ISO 27018	Incluso / Escluso
05 - Organizational controls	5.1	Politiche per la sicurezza delle informazioni	Policies for information security	X	X	Incluso
05 - Organizational controls	5.2	Ruoli e responsabilità in materia di sicurezza delle informazioni	Information security roles and responsibilities	X	X	Incluso
05 - Organizational controls	5.3	Segregazione dei compiti	Segregation of duties			Incluso
05 - Organizational controls	5.4	Responsabilità della Direzione	Management responsibilities			Incluso
05 - Organizational controls	5.5	Contatti con le autorità	Contact with authorities	X		Incluso
05 - Organizational controls	5.6	Contatto con gruppi di interesse specializzati	Contact with special interest groups			Incluso
05 - Organizational controls	5.7	Attività di "Threat intelligence"	Threat intelligence			Incluso
05 - Organizational controls	5.8	Sicurezza delle informazioni nella gestione dei progetti	Information security in project management	X		Incluso
05 - Organizational controls	5.9	Inventario delle informazioni e di altre attività associate	Inventory of information and other associated assets	X		Incluso

05 - Organizational controls	5.10	Uso accettabile delle informazioni e di altre risorse associate	Acceptable use of information and other associated assets			Incluso
05 - Organizational controls	5.11	Restituzione degli asset	Return of assets			Incluso
05 - Organizational controls	5.12	Classificazione delle informazioni	Classification of information			Incluso
05 - Organizational controls	5.13	Etichettatura delle informazioni	Labelling of information	X		Incluso
05 - Organizational controls	5.14	Trasferimento di informazioni	Information transfer		X	Incluso
05 - Organizational controls	5.15	Controllo di accesso	Access control	X	X	Incluso
05 - Organizational controls	5.16	Gestione delle identità	Identity management	X		Incluso
05 - Organizational controls	5.17	Informazioni di autenticazione	Authentication information	X		Incluso
05 - Organizational controls	5.18	Diritti di accesso	Access rights	X		Incluso
05 - Organizational controls	5.19	Sicurezza delle informazioni nei rapporti con i fornitori	Information security in supplier relationships	X		Incluso
05 - Organizational controls	5.20	Affrontare la sicurezza delle informazioni all'interno degli accordi con i fornitori	Addressing information security within supplier agreements	X		Incluso
05 - Organizational controls	5.21	Gestire la sicurezza delle informazioni nella catena di fornitura ICT	Managing information security in the ICT supply chain	X		Incluso

05 - Organizational controls	5.22	Monitoraggio, revisione e gestione del cambiamento dei servizi ai fornitori	Monitoring, review and change management of supplier services			Incluso
05 - Organizational controls	5.23	Sicurezza delle informazioni per l'utilizzo dei servizi cloud	Information security for use of cloud services			Incluso
05 - Organizational controls	5.24	Pianificazione e preparazione della gestione degli incidenti per la sicurezza delle informazioni	Information security incident management planning and preparation	X	X	Incluso
05 - Organizational controls	5.25	Valutazione e decisione sugli eventi di sicurezza delle informazioni	Assessment and decision on information security events			Incluso
05 - Organizational controls	5.26	Risposta agli incidenti di sicurezza delle informazioni	Response to information security incidents			Incluso
05 - Organizational controls	5.27	Imparare dagli incidenti di sicurezza delle informazioni	Learning from information security incidents			Incluso
05 - Organizational controls	5.28	Raccolta delle prove	Collection of evidence	X		Incluso
05 - Organizational controls	5.29	Sicurezza delle informazioni durante le interruzioni	Information security during disruption			Incluso
05 - Organizational controls	5.30	Preparazione ICT per la continuità aziendale	ICT readiness for business continuity			Incluso
05 - Organizational controls	5.31	Requisiti legali, statutari, normativi e contrattuali	Legal, statutory, regulatory and contractual requirements	X		Incluso
05 - Organizational controls	5.32	Diritti di proprietà intellettuale	Intellectual property rights	X	X	Incluso
05 - Organizational controls	5.33	Protezione dei dati	Protection of records	X		Incluso
05 - Organizational controls	5.34	Privacy e protezione delle PII	Privacy and protection of PII			Incluso

05 - Organizational controls	5.35	Revisione indipendente della sicurezza delle informazioni	Independent review of information security	X		Incluso
05 - Organizational controls	5.36	Conformità a politiche, regole e standard per la sicurezza delle informazioni	Compliance with policies, rules and standards for information security			Incluso
05 - Organizational controls	5.37	Procedure operative documentate	Documented operating procedures			Incluso
06 - People controls	6.1	Selezione	Screening			Incluso
06 - People controls	6.2	Condizioni di lavoro	Terms and conditions of employment			Incluso
06 - People controls	6.3	Sensibilizzazione, istruzione e formazione sulla sicurezza delle informazioni	Information security awareness, education and training	X	X	Incluso
06 - People controls	6.04	Processo disciplinare	Disciplinary process			Incluso
06 - People controls	6.05	Responsabilità dopo la cessazione o il cambiamento di rapporto di lavoro	Responsibilities after termination or change of employment			Incluso
06 - People controls	6.06	Accordi di riservatezza o non divulgazione	Confidentiality or non-disclosure agreements			Incluso
06 - People controls	6.07	Lavoro a distanza	Remote working			Incluso
06 - People controls	6.08	Segnalazione degli eventi di sicurezza delle informazioni	Information security event reporting	X		Incluso
07 - Physical controls	7.01	Perimetri di sicurezza fisica	Physical security perimeters			Incluso
07 - Physical controls	7.02	Ingresso fisico	Physical entry			Incluso
07 - Physical controls	7.03	Messa in sicurezza di uffici, camere e strutture	Securing offices, rooms and facilities			Incluso

07 - Physical controls	7.4	Monitoraggio della sicurezza fisica	Physical security monitoring			Incluso
07 - Physical controls	7.05	Protezione contro le minacce fisiche e ambientali	Protecting against physical and environmental threats			Incluso
07 - Physical controls	7.06	Lavorare in aree sicure	Working in secure areas			Incluso
07 - Physical controls	7.07	Scrivania chiara e schermo chiaro	Clear desk and clear screen			Incluso
07 - Physical controls	7.08	Ubicazione e protezione delle apparecchiature	Equipment siting and protection			Incluso
07 - Physical controls	7.09	Le attrezzature devono essere posizionate in modo sicuro e protetto.	Equipment shall be sited securely and protected.			Incluso
07 - Physical controls	7.10	Supporti di memorizzazione	Storage media			Incluso
07 - Physical controls	7.11	Utilità di supporto	Supporting utilities			Incluso
07 - Physical controls	7.12	Sicurezza del cablaggio	Cabling security			Incluso
07 - Physical controls	7.13	Manutenzione delle attrezzature	Equipment maintenance			Incluso
07 - Physical controls	7.14	Smaltimento sicuro o riutilizzo delle apparecchiature	Secure disposal or re-use of equipment	X	X	Incluso
08 - Technological controls	8.01	Dispositivi endpoint utente	User endpoint devices			Incluso
08 - Technological controls	8.02	Diritti di accesso privilegiato	Privileged access rights	X		Incluso
08 - Technological controls	8.03	Limitazione dell'accesso alle informazioni	Information access restriction	X		Incluso
08 - Technological controls	8.04	Accesso al codice sorgente	Access to source code			Incluso
08 - Technological controls	8.05	Autenticazione sicura	Secure authentication		X	Incluso

08 - Technological controls	8.06	Gestione della capacità	Capacity management	X		Incluso
08 - Technological controls	8.07	Protezione contro il malware	Protection against malware			Incluso
08 - Technological controls	8.08	Gestione delle vulnerabilità tecniche	Management of technical vulnerabilities	X		Incluso
08 - Technological controls	8.09	Gestione della configurazione	Configuration management			Incluso
08 - Technological controls	8.10	Cancellazione delle informazioni	Information deletion			Incluso
08 - Technological controls	8.11	Mascheramento dei dati	Data masking			Incluso
08 - Technological controls	8.12	Prevenzione della perdita di dati	Data leakage prevention			Incluso
08 - Technological controls	8.13	Backup delle informazioni	Information backup	X	X	Incluso
08 - Technological controls	8.14	Ridondanza delle strutture di elaborazione delle informazioni	Redundancy of information processing facilities			Incluso
08 - Technological controls	8.15	Registrazione	Logging	X	X	Incluso
08 - Technological controls	8.16	Attività di monitoraggio	Monitoring activities			Incluso
08 - Technological controls	8.17	Sincronizzazione dell'orologio	Clock synchronization	X		Incluso
08 - Technological controls	8.18	Utilizzo di programmi di utilità privilegiati	Use of privileged utility programs	X		Incluso
08 - Technological controls	8.19	Installazione di software su sistemi operativi	Installation of software on operational systems			Incluso
08 - Technological controls	8.20	Sicurezza delle reti	Networks security			Incluso
08 - Technological controls	8.21	Sicurezza dei servizi di rete	Security of network services			Incluso
08 - Technological controls	8.22	Segregazione delle reti	Segregation of networks	X		Incluso

08 - Technological controls	8.23	Attività di "Web filtering"	Web filtering			Incluso
08 - Technological controls	8.24	L'accesso a siti Web esterni dovrebbe essere gestito per ridurre l'esposizione a contenuti dannosi.	Access to external websites shall be managed to reduce exposure to malicious content.	X	X	Incluso
08 - Technological controls	8.25	Ciclo di vita dello sviluppo sicuro	Secure development life cycle	X		Incluso
08 - Technological controls	8.26	Requisiti di sicurezza delle applicazioni	Application security requirements			Incluso
08 - Technological controls	8.27	Architettura di sistema sicura e principi di progettazione	Secure system architecture and engineering principles			Incluso
08 - Technological controls	8.28	Codifica sicura	Secure coding			Incluso
08 - Technological controls	8.29	Test di sicurezza in fase di sviluppo e accettazione	Security testing in development and acceptance			Incluso
08 - Technological controls	8.30	Sviluppo in outsourcing	Outsourced development			Incluso
08 - Technological controls	8.31	Separazione degli ambienti di sviluppo, test e produzione	Separation of development, test and production environments		X	Incluso
08 - Technological controls	8.32	Gestione delle modifiche	Change management	X		Incluso
08 - Technological controls	8.33	Informazioni sul test	Test information			Incluso
08 - Technological controls	8.34	Protezione dei sistemi informativi durante i test di audit	Protection of information systems during audit testing			Incluso
ISO/IEC 27017:2015						
Relazione tra clienti di servizi cloud e provider di servizi cloud	**CLD.6.3.1**	Ruoli condivisi e responsabilità all'interno di un ambiente di cloud computing	**Shared roles and responsabilities within a computing environment**	X		Incluso

Responsabilità degli Asset	**CLD.8.1.5**	Rimozione delle risorse del cliente del servizio cloud	**Removal of cloud service customer assets**	X		Incluso
Controllo dell'accesso dei dati dei clienti del servizio cloud in un ambiente virtuale condiviso	**CLD.9.5.1**	Segregazione in ambienti di elaborazione virtuale	**Segregation in virtual computing environment**	X		Incluso
Controllo dell'accesso dei dati dei clienti del servizio cloud in un ambiente virtuale condiviso	**CLD.9.5.2**	Protezione avanzata della macchina virtuale	**Virtual machine hardening**	X		Incluso
Procedure e responsabilità operative	**CLD.12.1.5**	Sicurezza operativa dell'amministratore	**Administrator's operational security**	X		Incluso
Procedure e responsabilità operative	**CLD.12.4.5**	Monitoraggio del controllo dei servizi cloud	**Monitoring of cloud services**	X		Incluso
Gestione della sicurezza della rete	**CLD.13.1.4**	Allineamento della gestione della sicurezza per reti virtuali e fisiche	**Alignment of security management for virtual and physical networks**	X		Incluso
ISO/IEC 27018:2014						
Consenso e scelta	**A.2.1**	Obbligo di cooperare in materia dei principali diritti sul trattamento dei dati personali	*Obligation to co-operate regarding PII principals' rights*		X	Incluso
Legittimità dello scopo	**A.3.1**	Scopo del trattamento dei dati personali tramite public cloud	*Public cloud PII processor's purpose*		X	Incluso
Legittimità dello scopo	**A.3.2**	Uso commerciale dei del trattamento dei dati nel cloud pubblico	*Public cloud PII processor's commercial use*		X	Incluso
Minimizzazione dei Dati	**A.5.1**	Cancellazione sicura di file temporanei	*Secure erasure of temporary files*		X	Incluso
Limitazioni di utilizzo, conservazione e diffusione	**A.6.1**	Notifica dell'informativa di trattamento dei dati.	*PII disclosure notification*		X	Incluso
Limitazioni di utilizzo, conservazione e diffusione	**A.6.2**	Registrazione della diffusione dei dati personali.	*Recording of PII disclosures*		X	Incluso

Trasparenza e comunicazione	**A.8.1**	Comunicazione dell'utilizzo del subappalto per il trattamento dei dati personali	*Disclosure of sub-contracted PII processing*		X	Incluso
Accountability	**A.10.1**	Notifica di una violazione che coinvolga il trattamento di dati personali	*Notification of a data breach involving PII*		X	Incluso
Accountability	**A.10.2**	Periodo di conservazione per le politiche di sicurezza e le linee guida	*Retention period for administrative security policies and guidelines*		X	Incluso
Accountability	**A.10.3**	Restituzione, trasferimento e smaltimento dei dati personali	*PII return, transfer and disposal*		X	Incluso
Sicurezza delle Informazioni	**A.11.1**	Accordi di riservatezza o di non divulgazione	*Confidentiality or non-disclosure agreements*		X	Incluso
Sicurezza delle Informazioni	**A.11.2**	Limitazione della creazione di materiale cartaceo	*Restriction of the creation of hardcopy material*		X	Incluso
Sicurezza delle Informazioni	**A.11.3**	Controllo e la registrazione di ripristino dei dati	*Control and logging of data restoration*		X	Incluso
Sicurezza delle Informazioni	**A.11.4**	Protezione dei supporti di memorizzazione che escono dai locali	*Protecting data on storage media leaving the premises*		X	Incluso
Sicurezza delle Informazioni	**A.11.5**	L'utilizzo di supporti e dispositivi di memorizzazione portatili in chiaro (non cifrati)	*Use of unencrypted portable storage media and devices*		X	Incluso
Sicurezza delle Informazioni	**A.11.6**	Crittazione dei dati personali trasmessi su rete pubblica	*Encryption of PII transmitted over public data-transmission networks*		X	Incluso
Sicurezza delle Informazioni	**A.11.7**	Smaltimento sicuro dei materiali cartacei	*Secure disposal of hardcopy materials*		X	Incluso
Sicurezza delle Informazioni	**A.11.8**	Uso univoco di ID utente	*Unique use of user Ids*		X	Incluso
Sicurezza delle Informazioni	**A.11.9**	Registrazione di utenti autorizzati	*Records of authorized users*		X	Incluso
Sicurezza delle Informazioni	**A.11.10**	Gestione ID utenti	*User ID management*		X	Incluso

Sicurezza delle Informazioni	**A.11.11**	Misure contrattuali	*Contract measures*		X	Incluso
Sicurezza delle Informazioni	**A.11.12**	Contratti di trattamento dati con subappaltatori	*Sub-contracted PII processing*		X	Incluso
Sicurezza delle Informazioni	**A.11.13**	L'accesso ai dati su spazio usato precedentemente di archiviazione dati	*Access to data on pre-used data storage space*		X	Incluso
Privacy Compliance	**A.12.1**	Locazione geografica dei dati personali	*Geographical location of PII*		X	Incluso
Privacy Compliance	**A.12.2**	Destinazione dei dati personali	*Intended destination of PII*		X	Incluso