SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Piano di Trattamento del Rischio

EPTA TECH S.R.L. è una società italiana con sede legale a San Vito al Tagliamento (PN), operante nel settore dell'information technology, con attività prevalente di produzione e sviluppo di software non connesso all'edizione. L'azienda svolge attività di progettazione, realizzazione, commercializzazione, manutenzione e assistenza di soluzioni software, applicazioni web based, app e sistemi informatici, anche su commissione e su iniziativa propria.

La società opera inoltre nell'ambito della consulenza informatica, della gestione di servizi web, posta elettronica, hosting, housing, registrazione e mantenimento domini, nonché nella fornitura e gestione di servizi cloud quali SaaS, DaaS, HaaS, PaaS e IaaS. Rientrano inoltre nelle attività aziendali la realizzazione e gestione di siti internet, portali web, e-commerce, banche dati, reti dati, sistemi di telecomunicazione e soluzioni di sicurezza, sorveglianza e videosorveglianza.

In considerazione della natura delle attività svolte, EPTA TECH S.R.L. gestisce informazioni, infrastrutture tecnologiche, servizi digitali e ambienti cloud che richiedono adeguate misure di sicurezza, riservatezza, integrità, disponibilità e continuità operativa, in coerenza con i requisiti delle norme ISO/IEC 27001 e ISO/IEC 27017.

Codice	SGSI-TRT-001
Data documento	05/05/2026
Versione	00
Approvato da	Alta direzione

PRESENTAZIONE

Il presente documento è redatto per fornire una rappresentazione organica, elegante e professionale del Sistema di Gestione per la Sicurezza delle Informazioni dell'organizzazione, collegando business, asset, rischi, controlli, responsabilità e miglioramento continuo in un impianto coerente con la ISO/IEC 27001:2022.

SCOPO

Lo scopo del documento è supportare direzione, funzioni aziendali, auditor, consulenti e parti autorizzate nella comprensione del perimetro del SGSI, della logica di governo adottata, delle priorità di rischio e delle misure poste a presidio delle informazioni e dei servizi rilevanti.

DESCRIZIONE DELL'AZIENDA

EPTA TECH S.R.L. è una società italiana con sede legale a San Vito al Tagliamento (PN), operante nel settore dell'information technology, con attività prevalente di produzione e sviluppo di software non connesso all'edizione. L'azienda svolge attività di progettazione, realizzazione, commercializzazione, manutenzione e assistenza di soluzioni software, applicazioni web based, app e sistemi informatici, anche su commissione e su iniziativa propria.

La società opera inoltre nell'ambito della consulenza informatica, della gestione di servizi web, posta elettronica, hosting, housing, registrazione e mantenimento domini, nonché nella fornitura e gestione di servizi cloud quali SaaS, DaaS, HaaS, PaaS e IaaS. Rientrano inoltre nelle attività aziendali la realizzazione e gestione di siti internet, portali web, e-commerce, banche dati, reti dati, sistemi di telecomunicazione e soluzioni di sicurezza, sorveglianza e videosorveglianza.

In considerazione della natura delle attività svolte, EPTA TECH S.R.L. gestisce informazioni, infrastrutture tecnologiche, servizi digitali e ambienti cloud che richiedono adeguate misure di sicurezza, riservatezza, integrità, disponibilità e continuità operativa, in coerenza con i requisiti delle norme ISO/IEC 27001 e ISO/IEC 27017.

DESCRIZIONE DEL SERVIZIO

Il servizio di consulenza ha ad oggetto il supporto specialistico a EPTA TECH S.R.L. per la progettazione, implementazione, mantenimento e miglioramento di un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla norma ISO/IEC 27001, con estensione ai controlli e alle buone pratiche specifiche per i servizi cloud previste dalla ISO/IEC 27017.

L'attività comprende l'analisi del contesto aziendale, dei processi IT e cloud, delle infrastrutture tecnologiche, delle applicazioni software, dei servizi digitali erogati e delle informazioni trattate, al fine di individuare rischi, minacce, vulnerabilità e requisiti di sicurezza applicabili. La consulenza include inoltre il supporto nella definizione del campo di applicazione del sistema di gestione, nella valutazione dei rischi, nella redazione della documentazione richiesta, nella predisposizione delle procedure operative, nella selezione e applicazione dei controlli di sicurezza e nella preparazione all'eventuale audit di certificazione.

Particolare attenzione viene dedicata alla sicurezza dei servizi cloud, alla gestione delle responsabilità tra fornitore e cliente, alla protezione dei dati, al controllo degli accessi, alla continuità dei servizi, alla gestione degli incidenti, alla sicurezza delle infrastrutture, alla conformità normativa e contrattuale e al miglioramento continuo delle misure organizzative e tecniche adottate dall'azienda.

INDICE DEL DOCUMENTO

TERMINI IN USO

Termine	Definizione
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni.
Informazione	Dato o insieme di dati rilevanti per l'organizzazione, indipendentemente dal formato o supporto.
Asset	Qualsiasi risorsa informativa, organizzativa, tecnologica, fisica o di supporto rilevante per il SGSI.
Rischio	Effetto dell'incertezza sugli obiettivi, valutato in termini di probabilità e impatto.
Controllo	Misura organizzativa, fisica o tecnica adottata per modificare o presidiare il rischio.
Trattamento del rischio	Decisione e insieme di azioni per mitigare, trasferire, evitare o accettare un rischio.
SoA	Statement of Applicability: documento che riporta i controlli applicabili, il relativo stato e la giustificazione.
Parte interessata	Soggetto interno o esterno che può influenzare, essere influenzato o percepirsi influenzato dal SGSI.

PIANO DI TRATTAMENTO DEL RISCHIO

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Portale clienti / area riservata, con owner Responsabile IT / Commerciale e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT / Commerciale	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione	HR	2026-07-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.			
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Archivi cartacei riservati, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Amministrazione / Direzione	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Piattaforma documentale / DMS, con owner Qualità / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Qualità / IT	2026-07-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Marketing / IT	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Amministrazione / Direzione	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli	Marketing / IT	2026-07-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			organizzativi e tecnici proporzionati.			
Smarrimento o furto del dispositivo / Cifratura disco assente o controllo remoto non attivo		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Dispositivi mobili aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-06-04	planned
Smarrimento o furto del dispositivo / Cifratura disco assente o controllo remoto non attivo		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabili di funzione	2026-06-04	planned
Malware, ransomware o indisponibilità infrastrutturale / Patching incompleto, hardening insufficiente o monitoraggio debole		mitigate	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Workspace cloud collaborativo, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Malware, ransomware o indisponibilità infrastrutturale / Patching incompleto, hardening insufficiente o monitoraggio debole		mitigate	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned
Corruzione o modifica impropria dei dati / Mancanza di segregazione ruoli, log e controlli di integrità		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per CRM / ERP, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile di processo	2026-05-20	planned
Accesso non autorizzato ai dati / Credenziali deboli, MFA non attiva o privilegi eccessivi		mitigate	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per CRM / ERP, con owner Responsabile di processo e presidio del controllo	Responsabile di processo	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			Controlli organizzativi e tecnici proporzionati.			
Impossibilità di ripristino / Backup non testati o retention inadeguata		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned
Malware, ransomware o indisponibilità infrastrutturale / Patching incompleto, hardening insufficiente o monitoraggio debole		mitigate	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Server / infrastruttura virtuale, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Corruzione o modifica impropria dei dati / Mancanza di segregazione ruoli, log e controlli di integrità		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile commerciale / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile commerciale / IT	2026-05-20	planned
Accesso non autorizzato ai dati / Credenziali deboli, MFA non attiva o privilegi eccessivi		mitigate	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile commerciale / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile commerciale / IT	2026-05-20	planned
Phishing e compromissione account / Formazione insufficiente, MFA assente, filtri antispam non adeguati		mitigate	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights; A.6.3 Information security awareness, education and training; A.5.10 Acceptable use of information and other associated assets. Azione operativa suggerita: definire	Responsabile IT	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			attività, evidenze, verifiche e responsabilità per Caselle e-mail aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.			