SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Statement of Applicability

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-SOA-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.

DICHIARAZIONE DI APPLICABILITÀ

La seguente tabella riporta i controlli considerati nel perimetro SGSI, l’applicabilità, lo stato di implementazione e la relativa giustificazione.

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
A.5.1	Politiche per la sicurezza delle informazioni	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.2	Ruoli e responsabilità per la sicurezza delle informazioni	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.7	Threat intelligence	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.9	Inventario degli asset informativi	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
					associati e al piano di trattamento in essere.
A.5.10	Uso accettabile degli asset	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.12	Classificazione delle informazioni	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.15	Controllo degli accessi	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.18	Diritti di accesso	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.19	Sicurezza delle informazioni nei rapporti con i fornitori	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.23	Sicurezza per l’uso dei servizi cloud	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.24	Pianificazione della gestione incidenti	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.29	Sicurezza durante la disruption	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
A.5.30	ICT readiness per la continuità	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.6.3	Consapevolezza e formazione	Persone	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.6.5	Responsabilità a fine rapporto o cambio ruolo	Persone	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.1	Perimetri di sicurezza fisica	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.2	Controlli di accesso fisico	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.4	Monitoraggio sicurezza fisica	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.8	Collocazione e protezione apparecchiature	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.1	Dispositivi endpoint utente	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.2	Accessi privilegiati	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
					associati e al piano di trattamento in essere.
A.8.3	Restrizione accessi alle informazioni	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.5	Autenticazione sicura	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.8	Gestione vulnerabilità tecniche	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.9	Configuration management	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.10	Cancellazione delle informazioni	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.11	Data masking	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.12	Data leakage prevention	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.13	Backup delle informazioni	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
A.8.15	Logging	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.16	Monitoring activities	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.23	Web filtering	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.24	Uso della crittografia	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.