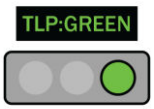
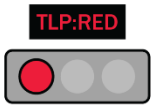
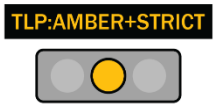
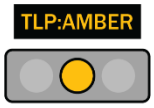
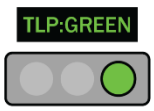
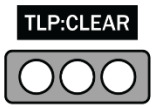
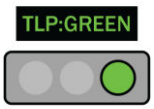
Versione Documento	1.0
Autore Documento	Fabio Finazzi
Data Documento	20/01/2025



Colore	Quando deve essere usato	Come deve essere condiviso
	Le fonti possono utilizzare TLP:RED quando non è possibile agire efficacemente sulle informazioni senza rischi significativi per la privacy, la reputazione o le operazioni delle organizzazioni coinvolte. Solo per gli occhi e le orecchie dei singoli destinatari, non oltre.	I destinatari non possono condividere le informazioni TLP:RED con alcuna parte al di fuori dello specifico scambio, incontro o conversazione in cui sono state originariamente divulgate. Nel contesto di una riunione, ad esempio, le informazioni TLP:RED sono limitate ai presenti alla riunione. Nella maggior parte dei casi, TLP:RED dovrebbe essere scambiato verbalmente o di persona.
	Le fonti possono utilizzare TLP:AMBER+STRICT quando le informazioni richiedono supporto per essere gestite in modo efficace, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise all'esterno dell'organizzazione.	I destinatari possono condividere le informazioni TLP:AMBER+STRICT solo con i membri della propria organizzazione in caso di necessità per proteggere la propria organizzazione e prevenire ulteriori danni.
	Le fonti possono utilizzare TLP:AMBER quando le informazioni richiedono supporto per essere gestite in modo efficace, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise al di fuori delle organizzazioni coinvolte. Tieni presente che TLP:AMBER+STRICT deve essere utilizzato per limitare la condivisione solo all'organizzazione destinataria.	I destinatari possono condividere le informazioni di TLP:AMBER con i membri della propria organizzazione e i suoi clienti in base alla necessità di sapere per proteggere la propria organizzazione e i suoi clienti e prevenire ulteriori danni.
	Le fonti possono utilizzare TLP:GREEN quando le informazioni sono utili per aumentare la consapevolezza all'interno della loro comunità più ampia.	I destinatari possono condividere le informazioni di TLP:GREEN con colleghi e organizzazioni partner all'interno della propria comunità, ma non tramite canali accessibili al pubblico. Se non diversamente specificato, le informazioni di TLP:GREEN non possono essere condivise al di fuori della comunità di sicurezza informatica o di difesa informatica.
	Le fonti possono utilizzare TLP:CLEAR quando le informazioni comportano un rischio minimo o non prevedibile di uso improprio, in conformità con le norme e le procedure applicabili per il rilascio al pubblico.	I destinatari possono condividere queste informazioni senza restrizioni. Le informazioni sono soggette alle norme standard sul copyright.

Versione Documento	1.0
Autore Documento	Fabio Finazzi
Data Documento	20/01/2025



Politica della Sicurezza delle Informazioni

Easytech SpA

---

1. Introduzione

La sicurezza delle informazioni è un aspetto fondamentale per garantire la continuità operativa, la protezione dei dati e la fiducia dei nostri stakeholder. La presente Politica della Sicurezza delle Informazioni definisce i principi, le responsabilità e le regole operative che devono essere seguiti all'interno dell'organizzazione per proteggere il patrimonio informativo, in accordo con i requisiti della norma **ISO/IEC 27001:2022**.

---

2. Scopo e Campo di Applicazione

2.1 Scopo

La politica ha lo scopo di:

- **Proteggere la riservatezza, integrità e disponibilità** delle informazioni aziendali.
- **Gestire i rischi** connessi alla sicurezza delle informazioni in modo sistematico.
- **Garantire la conformità** a normative, regolamenti interni ed esterni (ad es. GDPR, altre norme di settore).
- **Promuovere una cultura della sicurezza** all'interno dell'organizzazione.

2.2 Campo di Applicazione

La presente politica si applica a:

- Tutte le informazioni, indipendentemente dalla forma (documentale, elettronica, verbale, ecc.).
- Tutte le risorse informatiche e fisiche, nonché agli asset critici di business.
- Tutti i dipendenti, collaboratori, consulenti e terze parti che hanno accesso alle informazioni e alle risorse dell'organizzazione.

---

3. Principi di Sicurezza

L'organizzazione si impegna a garantire la sicurezza delle informazioni seguendo i seguenti principi:

- **Riservatezza:** Garantire che le informazioni siano accessibili solo alle persone autorizzate.
- **Integrità:** Salvaguardare l'accuratezza e la completezza delle informazioni e dei processi.
- **Disponibilità:** Assicurare che le informazioni e i sistemi siano disponibili agli utenti autorizzati quando necessario.
- **Tracciabilità e Controllo:** Mantenere registrazioni e log delle attività per consentire il monitoraggio e l'analisi degli eventi di sicurezza.
- **Conformità:** Rispettare le normative e i requisiti legali relativi alla protezione e gestione dei dati.

---

4. Ruoli e Responsabilità

4.1 Direzione

- Definire e approvare la politica e le strategie di sicurezza.
- Assegnare le risorse necessarie per l'implementazione e il mantenimento del Sistema di Gestione della Sicurezza delle Informazioni (ISMS).
- Promuovere la cultura della sicurezza in tutta l'organizzazione.

4.2 Responsabile della Sicurezza delle Informazioni (CISO)

- Coordinare lo sviluppo, l'implementazione e il monitoraggio della sicurezza delle informazioni.
- Gestire il processo di valutazione e mitigazione dei rischi.
- Assicurare la formazione e sensibilizzazione del personale in materia di sicurezza.

4.3 Proprietari delle Informazioni

- Assumersi la responsabilità di proteggere le informazioni sotto la loro gestione.
- Classificare e gestire le informazioni secondo i criteri definiti dalla politica interna.

4.4 Utenti e Collaboratori

- Rispettare le regole e le procedure di sicurezza.
- Segnalare tempestivamente eventuali incidenti o anomalie.
- Partecipare ai programmi di formazione e aggiornamento.

---

5. Gestione del Rischio e Misure di Sicurezza

5.1 Valutazione dei Rischi

- L'organizzazione effettuerà regolarmente valutazione dei rischi per identificare, valutare e mitigare le minacce e le vulnerabilità associate alle proprie informazioni e sistemi.
- I rischi saranno documentati e classificati in base al loro impatto e probabilità, adottando un approccio basato sul rischio.

5.2 Misure di Sicurezza Tecniche e Organizzative

- **Accesso e Controllo:** Implementazione di controlli di accesso fisici e logici per garantire che solo personale autorizzato acceda alle informazioni.
- **Protezione dei Dati:** Utilizzo di crittografia, backup regolari e altri strumenti di protezione per salvaguardare la riservatezza e l'integrità dei dati.
- **Monitoraggio e Log:** Implementazione di sistemi di monitoraggio (Sophos MDR) per rilevare tempestivamente eventuali incidenti di sicurezza.
- **Incident Response:** Predisposizione di procedure di gestione degli incidenti per una risposta rapida ed efficace in caso di violazioni o eventi critici.
- **Formazione e Sensibilizzazione:** Programmi di formazione continua per garantire che tutto il personale sia aggiornato sulle pratiche di sicurezza e sui rischi emergenti.

---

6. Conformità e Audit

- L'organizzazione effettuerà audit interni periodici per verificare l'efficacia delle misure implementate e la conformità della politica ai requisiti ISO/IEC 27001:2022.
- I risultati degli audit saranno oggetto di riesame e miglioramento continuo da parte della Direzione e del Responsabile della Sicurezza.

---

7. Gestione degli Incidenti

- Tutti gli incidenti di sicurezza dovranno essere immediatamente segnalati al Responsabile della Sicurezza delle Informazioni o al team dedicato, anche inviando una mail a supporto@easytechspa.com .
- Sarà predisposto un piano di Incident Response che definisce le azioni da intraprendere per contenere, analizzare e risolvere ogni evento critico.
- Le lezioni apprese saranno documentate e utilizzate per aggiornare le misure e prevenire future occorrenze.

---

8. Comunicazione e Revisione

- La presente politica sarà comunicata a tutti i livelli dell'organizzazione e resa disponibile a tutte le parti interessate.
- La politica verrà riesaminata almeno annualmente o in seguito a modifiche significative del contesto operativo o normativo, al fine di garantire la continua efficacia del Sistema di Gestione della Sicurezza delle Informazioni.

---

9. Sanzioni

- Il mancato rispetto della politica potrà comportare sanzioni disciplinari, fino alla cessazione del rapporto di lavoro, in conformità alle normative interne e alle disposizioni di legge vigenti.
- Le violazioni dovranno essere segnalate e saranno esaminate tramite appositi processi disciplinari e, se necessario, segnalate alle autorità competenti.

---

10. Conclusioni

L'organizzazione si impegna a mantenere elevati standard di sicurezza delle informazioni, proteggendo il patrimonio informativo e garantendo la continuità operativa e la fiducia dei propri stakeholder. La presente Politica della Sicurezza delle Informazioni costituisce un elemento chiave per il raggiungimento degli obiettivi di sicurezza aziendale e per il rispetto dei requisiti normativi, in particolare quelli previsti dalla norma ISO/IEC 27001:2022.

Fabio Finazzi

CISO – Easytech Group