

POLICY SICUREZZA INFORMAZIONI

Effegi Elettronica Srl

1 Controllo della versione del documento

	Ultima modifica	Ultima modifica di	Modifiche al documento
0.1	14/02/2025		Documento creato per la prima volta
0.2	11/01/2026	VOLA ANDREA	Firma Amm. Delegato / Revisione annuale

2 Indice

1	Controllo della versione del documento	1
2	Indice	2
3	Politica di sicurezza delle informazioni.....	4
3.1	Scopo	4
3.2	Destinatari	4
3.3	Principio	4
3.4	Dichiarazione di impegno degli amministratori delegati	4
3.5	introduzione	5
3.6	Obiettivi di sicurezza delle informazioni	5
3.7	Sicurezza delle informazioni definita	6
3.8	Quadro delle politiche di sicurezza delle informazioni	7
3.9	Ruoli e responsabilità della sicurezza delle informazioni	8
3.10	Monitoraggio	8
3.11	Obblighi legali e normativi	8
3.12	Formazione e consapevolezza	8

3.13	Miglioramento continuo del Sistema di Gestione	9
4	Conformità alle norme	9
4.1	Misurazione della conformità	9
4.2	Eccezioni	9
4.3	Inadempienza	9
4.4	Miglioramento continuo	10
5	Riferimenti controlli Annex A	11

3 Politica di sicurezza delle informazioni

3.1 Scopo

Lo scopo di questa politica è definire le politiche di sicurezza delle informazioni che si applicano all'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità dei dati.

3.2 Destinatari

Tutti i dipendenti e gli utenti terzi.

3.3 Principio

La sicurezza delle informazioni viene gestita in base al rischio, ai requisiti legali e normativi e alle esigenze aziendali.

3.4 Dichiarazione di impegno degli amministratori delegati

“Come azienda, l'elaborazione delle informazioni è fondamentale per il nostro successo e la protezione e la sicurezza di tali informazioni è una priorità a livello di consiglio di amministrazione. Che si tratti di informazioni sui dipendenti o informazioni sui clienti, prendiamo sul serio i nostri obblighi ai sensi del Regolamento Europeo 679/2016 (GDPR) e del D.Lgs.101/2018. Abbiamo fornito le risorse per sviluppare, implementare e migliorare continuamente la gestione della sicurezza delle informazioni adeguata alla nostra attività”.

Piercarlo Taverna - Amministratore

Effegi Elettronica Srl

Data: 11/01/2026

Firma: 

3.5 introduzione

La sicurezza delle informazioni protegge le informazioni che ci vengono affidate. Sbagliare la sicurezza delle informazioni può avere un impatto negativo significativo sui nostri dipendenti, sui nostri clienti, sulla nostra reputazione e sulle nostre finanze. Avendo un efficace sistema di gestione della sicurezza delle informazioni, siamo in grado di:

- Fornire garanzie per i nostri obblighi legali, normativi e contrattuali
- Assicurarci che le persone giuste abbiano il giusto accesso ai dati giusti al momento giusto
- Fornire protezione dei dati personali come definito dal GDPR
- Essere buoni custodi dei dati

3.6 Obiettivi di sicurezza delle informazioni

- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni dell'organizzazione, inclusi tutti i dati personali come definiti dal GDPR, sulla base di una buona gestione del rischio, degli obblighi normativi e contrattuali e delle esigenze aziendali.
- Fornire le risorse necessarie per sviluppare, implementare e migliorare continuamente il sistema di gestione della sicurezza delle informazioni.
- Gestire in modo efficace i fornitori di terze parti che elaborano, archiviano o trasmettono informazioni per ridurre e gestire i rischi per la sicurezza delle informazioni.
- Implementare una cultura della sicurezza delle informazioni e della protezione dei dati attraverso un'efficace formazione e sensibilizzazione.

3.7 Sicurezza delle informazioni definita

La sicurezza delle informazioni è definita come conservazione

Riservatezza	L'accesso alle informazioni è riservato a coloro che dispongono dell'autorità appropriata <i>Le persone giuste con l'accesso giusto</i>
Integrità	Le informazioni sono complete e accurate <i>ai dati giusti</i>
Disponibilità	Le informazioni sono disponibili quando sono necessarie <i>al momento giusto</i>

3.8 Quadro delle politiche di sicurezza delle informazioni

Il sistema di gestione della sicurezza delle informazioni è costruito su un insieme di politiche/policy di sicurezza delle informazioni.

- **DP 01 Politica sulla protezione dei dati**
- **DP 02 Politica di conservazione dei dati**
- **IS 01 Politica sulla sicurezza delle informazioni (questa politica)**
- **IS 02 Politica di controllo degli accessi**
- **IS 03 Politica di gestione patrimoniale**
- **IS 04 Politica di gestione dei rischi**
- **IS 05 Politica di classificazione e gestione delle informazioni**
- **IS 06 Politica di sensibilizzazione e formazione sulla sicurezza delle informazioni**
- **IS 07 Politica di utilizzo accettabile**
- **IS 08 Politica Clear Desk e Clear Screen**
- **IS 09 Politica in materia di mobilità e telelavoro**
- **IS 10 Politica di continuità operativa**
- **IS 11 Politica di backup**
- **IS 12 Politica antimalware e antivirus**
- **IS 13 Politica di gestione del cambiamento**
- **IS 14 Politica di sicurezza dei fornitori di terze parti**
- **IS 15 Politica di miglioramento continuo**
- **IS 16 Politica di registrazione e monitoraggio**
- **IS 17 Politica di gestione della sicurezza di rete**
- **IS 18 Politica di trasferimento delle informazioni**
- **IS 19 Politica di sviluppo sicuro**
- **IS 20 Politica di sicurezza fisica e ambientale**
- **IS 21 Politica di gestione delle chiavi crittografiche**
- **IS 22 Controllo crittografico e politica di crittografia**

- IS 23 **Politica sui documenti e registrazioni**
- IS 24 **Politica sugli incidenti significativi e raccolta di prove**
- IS 25 **Politica di gestione delle patch**
- IS 26 **Politica del servizio cloud**
- IS 27 **Politica sui diritti di proprietà intellettuale**

3.9 Ruoli e responsabilità della sicurezza delle informazioni

La sicurezza delle informazioni è responsabilità di tutti per comprendere e aderire alle politiche, seguire il processo e segnalare violazioni sospette o effettive. Specifici ruoli e responsabilità per la gestione del sistema di gestione della sicurezza delle informazioni sono definiti e registrati nel documento **Information Security Ruoli Assegnati e Responsabilità**

3.10 Monitoraggio

Il rispetto delle politiche e delle procedure del sistema di gestione della sicurezza delle informazioni è monitorato tramite il Management Review Team, insieme a revisioni indipendenti da parte sia dell'Internal che dell'External Audit su base periodica.

3.11 Obblighi legali e normativi

L'organizzazione prende sul serio i propri obblighi legali e normativi e tali requisiti sono registrati nel documento Terms & Conditions che rappresenta una sorta di registro dei requisiti legali e contrattuali

3.12 Formazione e consapevolezza

Le politiche sono rese prontamente e facilmente disponibili a tutti i dipendenti e agli utenti di terze parti. È in atto un piano di formazione e comunicazione per comunicare le politiche, il processo e i concetti di sicurezza delle informazioni. Le esigenze di

formazione sono identificate e i requisiti di formazione pertinenti sono registrati nel documento **Matrice delle competenze**.

3.13 Miglioramento continuo del Sistema di Gestione

Il sistema di gestione della sicurezza delle informazioni viene continuamente migliorato. La **politica di miglioramento continuo** definisce l'approccio aziendale al miglioramento continuo ed è in atto un processo di miglioramento continuo.

4 Conformità alle norme

4.1 Misurazione della conformità

Il team di gestione della sicurezza delle informazioni verificherà la conformità a questa politica attraverso vari metodi, inclusi, a titolo esemplificativo ma non esaustivo, rapporti sugli strumenti aziendali, audit interni ed esterni e feedback al proprietario della politica.

4.2 Eccezioni

Qualsiasi eccezione alla politica deve essere approvata e registrata dal responsabile della sicurezza delle informazioni in anticipo e segnalata al team di revisione della direzione.

4.3 Inadempienza

Un dipendente scoperto ad aver violato questa politica può essere soggetto ad azione disciplinare, fino al licenziamento incluso.

4.4 Miglioramento continuo

La politica viene aggiornata e rivista come parte del processo di miglioramento continuo.

5 Riferimenti controlli Annex A

ISO27001:2022	ISO27002:2022	ISO27001:2013/2017	ISO27002:2013/2017
ISO27001:2022 Clausola 5 Leadership	ISO27002:2022 Clausola 5 Controlli organizzativi	ISO27001:2013/2017 Clausola 5 Leadership	ISO27002:2013/2017 Clausola 5 Politiche di sicurezza delle informazioni
ISO27001:2022 Clausola 5.1 Leadership e impegno	ISO27002:2022 Clausola 5.1 Politiche per la sicurezza delle informazioni	ISO27001:2013/2017 Clausola 5.1 Leadership e impegno	ISO27002:2013/2017 Clausola 5.1 Direzione della direzione per la sicurezza delle informazioni
ISO27001:2022 Clausola 5.2 Politica	ISO27002:2022 Clausola 5.36 Conformità a politiche, regole e standard per la sicurezza delle informazioni	ISO27001:2013/2017 Clausola 5.2 Politica	ISO27002:2013/2017 Clausola 5.1.1 Politiche per la sicurezza delle informazioni
ISO27001:2022 Clausola 6.2 Obiettivi di sicurezza delle informazioni e pianificazione per raggiungerli	ISO27002:2022 Clausola 5.4 Responsabilità della direzione	ISO27001:2013/2017 Clausola 6.2 Obiettivi di sicurezza delle informazioni e pianificazione per raggiungerli	ISO27002:2013/2017 Clausola 5.1.2 Revisione delle politiche per la sicurezza delle informazioni
ISO27001:2022 Clausola 7.3 Consapevolezza	ISO27002:2022 Clausola 6 Controlli sulle persone	ISO27001:2013/2017 Clausola 7.3 Consapevolezza	ISO27002:2013/2017 Clausola 7 Sicurezza delle risorse umane
	ISO27002:2022 Clausola 6.3 Consapevolezza, istruzione e formazione sulla sicurezza delle informazioni		ISO27002:2013/2017 Clausola 7.2.1 Responsabilità della direzione
	ISO27002:2022 Clausola 6.4 Processo disciplinare		ISO27002:2013/2017 Clausola 7.2.2 Consapevolezza, istruzione e formazione sulla sicurezza delle informazioni
			ISO27002:2013/2017 Clausola 7.2.3 Processo disciplinare