TLP:CLEAR

Divulgazione illimitata

Centro Papa Giovanni XXIII

Via Madre Teresa di Calcutta, 1, 60131, Ancona (AN)

Tel: 0712140199

E mail: info@centropapagiovanni.it

Pec: centropapagiovannicoopsoc@pec.confcooperative.it

POLITICA PER LA SICUREZZA INFORMATICA

(in conformità al D.Lgs. 138/2024 e alle Linee guida ACN – Specifiche di base NIS)

Approvato dall'Organo di Amministrazione ai sensi dell'art. 23 del D.Lgs. 138/2024.

Data di approvazione: *23/02/2026*
Approvato da: *Giorgia Sordoni*
Ruolo: Presidente / Amministratore Delegato
Versione: 1.0 del *23/02/2026*

TLP:CLEAR

Divulgazione illimitata

Sommario

1. Premessa e dichiarazione di impegno 3
2. Ambito di applicazione 3
3. Quadro normativo e di riferimento 3
4. Principi generali di sicurezza informatica 4
5. Misure di sicurezza di base 4
6. Approccio basato sul rischio 5
7. Gestione degli incidenti 5
8. Continuità operativa e disaster recovery 5
9. Sicurezza della supply chain 6
10. Documentazione e controlli 6
11. Formazione e cultura della sicurezza 7
12. Monitoraggio e miglioramento continuo 7
13. Conclusioni 7

TLP:CLEAR

Divulgazione illimitata

1. Premessa e dichiarazione di impegno

L'Azienda riconosce che la cybersicurezza non è un elemento accessorio ma un pilastro strategico della propria operatività e del valore che genera per i clienti, gli utenti e la collettività. Con questa politica, l'Azienda si assume l'impegno formale di conformarsi al Decreto Legislativo 4 settembre 2024 n. 138 ("Decreto NIS2") e alle linee guida e alle "Specifiche di base" elaborate dall'Agenzia per la Cybersicurezza Nazionale (ACN). L'obiettivo è garantire un livello elevato e comune di sicurezza informatica, tutelando la disponibilità, la riservatezza e l'integrità dei sistemi informativi, delle infrastrutture digitali e dei dati che supportano le attività aziendali.

2. Ambito di applicazione

La presente politica si applica all'intera organizzazione, includendo tutti i sistemi informativi e di rete utilizzati dall'Azienda per lo svolgimento delle proprie attività e la prestazione dei servizi ad essa affidati. Essa coinvolge tutto il personale – interno, dipendente o collaboratore – nonché i soggetti esterni (fornitori, partner, sub-fornitori, consulenti) che, in qualunque misura, accedono o gestiscono risorse ICT aziendali. La politica è rivolta in particolare a quei servizi che, in base al Decreto NIS2, rientrano nella categoria dei "servizi essenziali" o "servizi importanti", intendendosi per questi quei processi e infrastrutture il cui malfunzionamento o compromissione potrebbe generare conseguenze rilevanti per la continuità operativa, la sicurezza e il corretto funzionamento del sistema economico e sociale.

3. Quadro normativo e di riferimento

L'Azienda riconosce che questa politica si fonda su un quadro normativo e di best-practice articolato e vincolante. In particolare, fa riferimento al D.Lgs. 138/2024, che recepisce la direttiva (UE) 2022/2555 (nota come NIS 2) nel nostro ordinamento nazionale. Inoltre, prende atto delle indicazioni emanate dall'ACN mediante le "Specifiche di base" approvate con determinazione n. 164179/2025, che definiscono le misure minime di sicurezza tecnico-organizzativa applicabili. A complemento, l'Azienda si ispira a standard internazionali riconosciuti (ad esempio gli standard della famiglia ISO/IEC 27000) e ai principi di governance, gestione del rischio e continuità operativa. La politica si fonda sul D.Lgs. 138/2024, che recepisce la Direttiva (UE) 2022/2555 (NIS2) nel nostro ordinamento, e sulle Specifiche di base approvate da ACN con determinazione n. 164179 del 14 aprile 2025. Essa si ispira inoltre a standard internazionali come ISO/IEC 27001, 27035, 22301 e 31000.

4. Principi generali di sicurezza informatica

La politica aziendale si fonda su principi di governance chiara, approccio basato sul rischio, proporzionalità delle misure, prevenzione e resilienza, miglioramento continuo e tracciabilità di ogni decisione e azione di sicurezza informatica intesi come qui di seguito:

- **Governance e responsabilità chiare**: l'organo di amministrazione e i vertici aziendali assumono la responsabilità ultima della sicurezza informatica, garantendo che siano definiti ruoli, responsabilità e obblighi in modo trasparente e documentato.

- **Approccio basato sul rischio**: ogni decisione relativa alla sicurezza – dalle infrastrutture ai processi, dai fornitori al personale – è presa tenendo conto della natura, probabilità e impatto dei rischi, con un'attitudine proattiva più che reattiva.

- **Proporzionalità ed adeguatezza:** le misure tecnico-organizzative sono calibrate in modo tale da risultare adeguate al livello di rischio effettivo, alla dimensione aziendale, alla complessità dei sistemi e all'ambito di attività.

- **Prevenzione e resilienza**: non basta reagire agli incidenti, ma occorre dotarsi di misure preventive, monitoraggio continuo, capacità di risposta e recupero rapido, così da garantire la continuità delle attività in scenari avversi.

- **Miglioramento continuo**: la sicurezza informatica non è un traguardo statico ma un processo in evoluzione: le misure, i processi e i sistemi devono essere periodicamente riesaminati, testati e aggiornati per tenere il passo con il mutare delle minacce, delle tecnologie e del contesto aziendale.

- **Trasparenza, tracciabilità e documentazione**: tutte le decisioni, le azioni, gli strumenti e gli eventi significativi in ambito sicurezza informatica sono documentati, monitorati, verificabili e soggetti ad audit, così da garantire evidenza e responsabilità.

5. Misure di sicurezza di base

L'Azienda attua misure di sicurezza articolate nelle funzioni di governance, identificazione, protezione, rilevazione, risposta e ripristino, come previste dalle Specifiche di base ACN e dal Decreto NIS2. Esse comprendono l'adozione di politiche, la gestione del rischio, i controlli di accesso, la cifratura dei dati, il monitoraggio degli eventi e la predisposizione di piani di risposta e continuità.

6. Approccio basato sul rischio

L'Azienda individua i sistemi informativi e di rete che rivestono rilevanza strategica (ossia quei sistemi la cui compromissione può generare conseguenze elevate in termini di disponibilità, integrità o riservatezza). Sulla base di questa individuazione, l'Azienda svolge valutazioni periodiche del rischio, producendo una mappatura chiara delle minacce, delle vulnerabilità, delle conseguenze e del livello di esposizione. A seguito di questa valutazione, viene predisposto un piano di trattamento del rischio che include sia misure preventive che compensative. Le decisioni di investimento, di scelta dei fornitori, di sviluppo dei sistemi e di gestione del ciclo di vita dei prodotti devono incorporare la dimensione del rischio cyber, affinché la sicurezza informatica sia integrata nel business e non relegata a una funzione in isolamento.

7. Gestione degli incidenti

L'Azienda considera che la capacità di gestire prontamente un incidente informatico è tanto importante quanto la prevenzione. Per questo motivo, è stato definito un piano operativo per la gestione degli incidenti di sicurezza informatica, che prevede: innanzitutto, l'identificazione tempestiva dell'evento, la sua registrazione, la valutazione immediata dell'impatto e della potenziale diffusione, l'attivazione dei flussi decisionali interni e del comitato crisi aziendale, la notifica al CSIRT Italia (funzione operativa presso l'ACN) nei tempi e nelle modalità stabilite dal Decreto NIS2. Ad esempio, entro 24 ore dalla conoscenza dell'incidente per la "pre-notifica", e entro 72 ore per la notifica completa, laddove l'impatto sull'erogazione dei servizi sia significativo. Durante la fase di risposta, l'Azienda interviene per contenere la diffusione, ripristinare i servizi e raccogliere le evidenze utili per l'analisi forense. Al termine dell'evento, è prevista una fase di revisione, lezione appresa, aggiornamento dei piani e comunicazione interna ed esterna se necessario.

8. Continuità operativa e disaster recovery

L'Azienda mantiene e aggiorna un Piano di continuità operativa e di disaster recovery che include procedure di backup, test di ripristino e gestione delle crisi. I piani sono approvati dagli organi di amministrazione e aggiornati annualmente.

9. Sicurezza della supply chain

L'Azienda riconosce che la propria sicurezza dipende anche dalla sicurezza dei fornitori, partner e sub-fornitori che partecipano alla catena ICT. Pertanto, nei rapporti contrattuali con soggetti che erogano servizi o forniscono componenti rilevanti per la sicurezza informatica, l'Azienda può inserisce clausole specifiche di conformità alla presente politica e alle normative applicabili. Il processo di selezione, qualificazione e monitoraggio dei fornitori prevede la valutazione della loro postura di sicurezza, della compliance normativa, della gestione delle vulnerabilità, e della capacità di rispondere ad incidenti. Vengono tenuti registri dei fornitori ICT rilevanti, flussi informativi e rapporti contrattuali che prevedono obblighi di continuità, segnalazione incidenti e audit. Questo approccio alla supply chain fa parte integrante del programma di sicurezza aziendale.

10. Documentazione e controlli

Tutte le attività di sicurezza sono documentate in modo completo e verificabile. Sono mantenuti inventari, registri, piani e procedure approvate dal CdA o equivalente. Vengono eseguite verifiche periodiche per verificare la conformità e l'efficacia delle misure di sicurezza.

Di seguito la sintesi:

- Inventari di asset, software, reti e fornitori;
- Elenchi del personale di sicurezza e delle configurazioni di riferimento;
- Piani di rischio, continuità, formazione e incident response;
- Procedure e registri di audit e formazione;
- Politiche di sicurezza informatica approvate dal CdA (GV.PO-01).

Tutti i documenti sono revisionati almeno annualmente e approvati dagli organi di amministrazione e direttivi, come da Appendice C delle Linee guida ACN.

11. Formazione e cultura della sicurezza

L'Azienda promuove la consapevolezza del personale attraverso un piano di formazione sulla sicurezza informatica, rivolto a tutto il personale e agli organi direttivi, in linea con l'obbligo normativo. La cultura della sicurezza può essere promossa mediante comunicazioni, workshop, test di simulazione e verifiche di apprendimento.

12. Monitoraggio e miglioramento continuo

Almeno una volta l'anno, oppure in caso di eventi significativi (ad esempio cambiamenti normativi, incidenti rilevanti, modifiche infrastrutturali/organizzative), il programma di sicurezza viene riesaminato, gli obiettivi aggiornati, le risorse adeguate e le azioni correttive approvate dalla direzione. L'obiettivo è assicurare non solo il mantenimento della conformità, ma un percorso di miglioramento continuo della postura di sicurezza della società.

13. Conclusioni

Con la presente politica, l'Azienda afferma il proprio impegno a conformarsi pienamente al D.Lgs. 138/2024 e alle Linee guida ACN. La sicurezza informatica è parte integrante della cultura aziendale e della responsabilità verso i clienti, i partner e la collettività.