

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

In conformità alla norma ISO 27001:2022 e Direttiva (UE) 2022/2555 – NIS2

1. PREMESSA

Lo scopo della presente politica è descrivere i principi generali di sicurezza delle informazioni definiti da CASSIOLI S.r.l. per promuovere un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni ai sensi della normativa ISO/IEC 27001:2022 e della Direttiva (UE) 2022/2555 – NIS2, in particolare gli articoli 21, 23 e 26 relativi alle misure tecniche e organizzative, gestione del rischio, sicurezza della supply chain e gestione degli incidenti.

2. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

CASSIOLI S.r.l. ha come obiettivo primario la protezione dei dati, della struttura tecnologica, fisica, logica ed organizzativa, tale condizione potrà essere raggiunta, attraverso il rispetto dei seguenti principi:

- a) **Riservatezza:** garantire che le informazioni siano accessibili solo a soggetti autorizzati, mediante controlli di accesso, classificazione delle informazioni e misure tecniche adeguate.;
- b) **Integrità:** assicurare che le informazioni siano accurate, complete e protette da modifiche non autorizzate.;
- c) **Disponibilità:** garantire che le informazioni e i servizi siano accessibili quando necessario, attraverso misure di continuità operativa e resilienza.;
- d) **Controllo:** assicurare che i processi di gestione delle informazioni siano strutturati, documentati, verificabili e supportati da strumenti sicuri e testati.;

Nell'ambito della gestione dei servizi offerti, CASSIOLI S.r.l. attraverso la propria infrastruttura tecnologica, assicura:

- a) il rispetto delle normative vigenti e degli standard internazionali di sicurezza;
- b) la selezione di partner affidabili, valutati anche secondo i requisiti di sicurezza della supply chain;
- c) la completa osservanza dei livelli di servizio stabiliti con i clienti; d) la soddisfazione del cliente e l'erogazione di servizi con elevati standard qualitativi;
- d) l'adozione di misure tecniche e organizzative adeguate alla gestione del rischio;
- e) la capacità di prevenire, rilevare, gestire e comunicare incidenti di sicurezza;

Per questo motivo CASSIOLI S.r.l. ha sviluppato un sistema di gestione delle informazioni che rispetta i requisiti previsti dalla Norma ISO 27001:2022 e dalle leggi vigenti al fine di gestire la sicurezza delle informazioni nell'ambito della propria attività;

La politica per la sicurezza delle informazioni di CASSIOLI S.r.l. si applica a tutto il personale interno ed alle terze parti (es: fornitori di servizi, collaboratori, addetti alle manutenzioni) che collaborano con CASSIOLI S.r.l. alla gestione delle informazioni ed a tutti i processi e alle risorse coinvolte nei processi di progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

CASSIOLI S.r.l. ha formalizzato, mediante apposite nomine, il mansionario e l'organigramma aziendale, i ruoli e le responsabilità in materia di sicurezza delle informazioni, tra cui l'Amministratore di Sistema (AdS), il CISO, il Referente CSIRT, il Data Protection Officer (DPO) e il Punto di contatto, garantendo un'adeguata separazione dei compiti (a titolo di esempio, gli audit interni sono affidati a una società esterna al fine di assicurarne l'imparzialità).

La presente politica, unitamente a tutte le politiche ad essa connesse, è approvata dal Consiglio di amministrazione, viene condivisa con il personale mediante pubblicazione sul sito aziendale ed è oggetto di revisione con cadenza almeno annuale in sede di riesame della Direzione.

La presente politica è attuata attraverso le procedure di sistema del SGSI (PRO.SGSI.01 ÷ PRO.SGSI.07) e le politiche specifiche ad essa connesse (POL.SGSI_02 Fornitori, POL.SGSI_03 Controllo accessi logici, POL.SGSI_04 Intelligenza Artificiale), condivise con il personale tramite il canale Teams aziendale.

CASSIOLI S.r.l. definisce e riasamina almeno annualmente:

- il contesto interno ed esterno;
- le parti interessate;
- i rischi e le opportunità relativi alla sicurezza delle informazioni;

- i rischi relativi alla continuità operativa e alla resilienza dei servizi essenziali (NIS2 art. 21(2)(e))
- i rischi derivanti dalla supply chain e dai fornitori critici (NIS2 art. 21(2)(b))

La politica della sicurezza delle informazioni di CASSIOLI S.r.l. rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di CASSIOLI S.r.l. si ispira ai seguenti principi:

- garantire il controllo degli accessi alle informazioni aziendali ed ai dati trattati;
- stabilire la classificazione e il trattamento delle informazioni;
- garantire la sicurezza fisica dei luoghi di lavoro e delle attrezzature in essi contenuti;
- adottare politiche di gestione atte a massimizzare la sicurezza delle informazioni trattate quali ad esempio:
 - ✓ corretto uso degli asset aziendali;
 - ✓ favorire e stimolare buone pratiche inerenti alla riservatezza delle informazioni (scrivania ordinata e modalità di archiviazione anonima delle informazioni su PC);
 - ✓ adeguato trasferimento delle informazioni;
 - ✓ uso regolamentato dei dispositivi mobili e telelavoro;
 - ✓ limitazioni all'installazione e all'utilizzo di software;
 - ✓ Navigazione sicura verso i siti consentiti;
- stabilire ed effettuare backup sulla base di regole indicate dalla direzione secondo logiche di pianificazione temporale (intervalli regolari);
- stabilire procedure per il trasferimento di informazioni in modo protetto;
- prevedere protezioni dai malware;
- individuare, monitorare e gestire le vulnerabilità tecniche riscontrate;
- prevedere, se necessario, controlli crittografici;
- garantire la sicurezza delle comunicazioni;
- rispettare le normative vigenti in ambito Privacy e protezione dei dati personali;
- Intrattenere rapporti con i fornitori in ottica ISO/IEC 27001 e NIS2;
- la selezione di partner affidabili, valutati anche secondo i requisiti di sicurezza della supply chain;
- la capacità di prevenire, rilevare, gestire e comunicare incidenti di sicurezza;

La presente politica fa riferimento alle attività svolte da CASSIOLI S.r.l. in materia di:

“Progettazione, sviluppo, realizzazione, installazione e manutenzione di sistemi di automazione industriale e intralogistica – inclusi magazzini automatici, sistemi AGV/AMR, linee di montaggio e soluzioni di movimentazione merci – per clienti livello nazionale e internazionale.”

Torrita di Siena, 05/08/2026

Rev.0


La Direzione