Displaid

MOD 520

Politica del Sistema di Gestione delle Informazioni

DISPLAID S.R.L. SOCIETÀ BENEFIT
VIA CARLO FREGUGLIA, 2 20122 MILANO
PARTITA IVA.: 12832220961

Indice

1. Scopo 3
2. Campo di applicazione 3
3. Riferimenti normativi 4
4. Termini e definizioni 4
5. Ruoli e responsabilità 4
6. Impegno e obiettivi del sistema di gestione 5
6.1 Impegno della Direzione 5
6.2 Obiettivi di sicurezza delle informazioni 6
6.3 Comunicazione e diffusione della politica 6
7. Archiviazione e aggiornamento 7
8. Documenti di riferimento 7

Storico versione documento

VERSIONE	DATA	AUTORE	APPROVATO DA
1	08/06/2026	Francesco Morgan Bono	Lorenzo Benedetti

Politica del Sistema di Gestione delle Informazioni

1. Scopo

Displaid S.r.l. Società Benefit riconosce la protezione delle informazioni come presupposto essenziale per perseguire la propria missione nel campo del monitoraggio strutturale di infrastrutture critiche. L'attività dell'organizzazione, che comprende la progettazione di hardware IoT proprietario, lo sviluppo di algoritmi diagnostici basati sull'intelligenza artificiale e l'erogazione del servizio di monitoraggio attraverso la piattaforma Iris, genera, elabora e conserva dati la cui riservatezza, integrità e disponibilità sono determinanti tanto per la sicurezza delle opere monitorate quanto per la fiducia dei committenti pubblici e privati.

La presente politica esprime la volontà dell'Alta Direzione di tutelare gli asset informativi aziendali e di orientare il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) verso obiettivi coerenti con il contesto operativo, il modello di business e gli indirizzi strategici di Displaid. Il documento costituisce il quadro di riferimento per la definizione e il riesame degli obiettivi di sicurezza delle informazioni, formalizza l'impegno a soddisfare i requisiti applicabili e promuove il miglioramento continuo dell'efficacia del SGSI, in armonia con la natura di Società Benefit dell'organizzazione e con la responsabilità che essa avverte verso le proprie parti interessate.

2. Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici di Displaid S.r.l. Società Benefit, con riferimento alla sede legale in Via Carlo Freguglia 2, 20122 Milano (MI) e alla sede operativa in Via Colico 36, 20158 Milano (MI). Sono destinatari del documento tutti i dipendenti, i collaboratori, i consulenti, gli appaltatori e i soggetti terzi che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla sede di lavoro. Il perimetro comprende l'intero ciclo di progettazione, sviluppo, installazione ed erogazione dei sistemi di monitoraggio strutturale e dei servizi di analisi dati associati, nonché le attività amministrative e direzionali di supporto.

3. Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27000:2018
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003

4. Termini e definizioni

- **Sicurezza delle informazioni:** preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Sistema di gestione della sicurezza delle informazioni:** componente del sistema di gestione complessivo, basata su un approccio al rischio, volta a stabilire, attuare, gestire, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.
- **Politica:** intenzioni e orientamento di un'organizzazione espressi formalmente dalla sua Alta Direzione.
- **Parte interessata:** persona o organizzazione che può influenzare, essere influenzata o percepirsi come influenzata da una decisione o da un'attività.
- **Miglioramento continuo:** attività ricorrente finalizzata ad accrescere le prestazioni.

5. Ruoli e responsabilità

- **AD:** stabilisce, approva e mantiene aggiornata la presente politica, garantendone la coerenza con il contesto organizzativo e gli indirizzi strategici dell'azienda.
- **Responsabile del Sistema di Gestione:** supporta l'**AD** nella redazione della politica, ne verifica l'allineamento con l'analisi del contesto e la valutazione dei rischi, e coordina l'attuazione degli impegni di sicurezza delle informazioni.
- **RGQ:** cura la formalizzazione, il controllo delle revisioni e la distribuzione della politica al personale e alle parti interessate attraverso i canali aziendali autorizzati.
- **DS:** contribuisce alla definizione degli indirizzi strategici che orientano la politica e ne promuove l'applicazione nei rapporti istituzionali e commerciali.
- **RDP Produzione:** assicura l'integrazione dei principi espressi dalla politica nei processi di produzione e consegna dei sistemi di monitoraggio.
- **RDP Supporto:** garantisce l'applicazione degli impegni di sicurezza nelle attività di supporto tecnico, installazione sul campo e manutenzione.
- **RDP Amministrazione:** verifica il rispetto dei requisiti di sicurezza delle informazioni nei processi amministrativi, contrattuali e nella gestione dei rapporti con i fornitori.

6. Impegno e obiettivi del sistema di gestione

6.1 Impegno della Direzione

L'Alta Direzione di Displaid, consapevole del valore strategico che la sicurezza delle informazioni riveste per un'azienda deep-tech impegnata nel monitoraggio di ponti, viadotti e infrastrutture critiche, assume con la presente politica impegni vincolanti verso la protezione del patrimonio informativo aziendale.

L'organizzazione promuove una cultura della sicurezza fondata sulla responsabilità condivisa, nella quale ogni persona che interagisce con i dati e i sistemi aziendali è consapevole del proprio ruolo nella tutela delle informazioni. L' **AD** destina le risorse finanziarie, umane e tecnologiche necessarie a sostenere il SGSI e a integrare i requisiti di sicurezza in ogni processo: dalla progettazione degli Smart Sensor e degli algoritmi diagnostici all'erogazione del servizio di monitoraggio attraverso la piattaforma Iris, fino alle attività amministrative e ai rapporti con le terze parti. Le modalità operative attraverso cui l'Alta Direzione esercita la leadership e il governo del SGSI sono dettagliate nella *PRO Processi direzionali*.

Displaid adotta un approccio sistematico orientato al rischio, nel quale le decisioni di sicurezza sono proporzionate al livello di rischio valutato e il rischio residuo è mantenuto entro la soglia di accettabilità definita dall'organizzazione. Le modalità di identificazione, valutazione e trattamento dei rischi sono descritte nella *PRO Procedura di gestione dei rischi*, i cui esiti alimentano la definizione delle priorità e delle misure di protezione.

L'azienda si impegna a soddisfare i requisiti applicabili di natura legislativa, regolamentare e contrattuale, con particolare attenzione alla protezione dei dati personali e agli obblighi derivanti dai rapporti con le pubbliche amministrazioni committenti. Il rispetto della normativa vigente e degli impegni assunti verso clienti, fornitori, investitori e autorità di controllo costituisce una condizione essenziale per la sostenibilità e la credibilità del modello di business dell'organizzazione. I principi fondamentali di sicurezza che guidano tutte le policy e le procedure operative sono definiti nella *POL Politica di sicurezza delle informazioni.*

Il perseguimento del miglioramento continuo permea l'intero SGSI: attraverso l'analisi degli incidenti, le valutazioni periodiche dei rischi, gli audit interni e i riesami della direzione, Displaid identifica costantemente le opportunità per rafforzare i propri controlli e accrescere l'efficacia delle misure di protezione adottate.

6.2 Obiettivi di sicurezza delle informazioni

Il presente documento fornisce il quadro di riferimento per la definizione, il riesame e l'aggiornamento degli obiettivi di sicurezza delle informazioni. L'organizzazione persegue i seguenti obiettivi strategici, coerenti con il proprio contesto e con gli indirizzi dell'Alta Direzione:

- Proteggere la riservatezza, l'integrità e la disponibilità dei dati di telemetria acquisiti dagli Smart Sensor, degli algoritmi diagnostici proprietari e di tutte le informazioni trattate attraverso la piattaforma Iris e l'infrastruttura cloud.
- Mantenere il rischio residuo entro un livello accettabile, applicando misure di trattamento proporzionate alla criticità degli asset e al contesto operativo dell'organizzazione.
- Soddisfare i requisiti legislativi, regolamentari e contrattuali applicabili, con specifico riguardo alla protezione dei dati personali e agli obblighi nei confronti delle pubbliche amministrazioni committenti.
- Rafforzare la consapevolezza in materia di sicurezza delle informazioni presso tutto il personale, attraverso programmi di formazione e sensibilizzazione adeguati ai diversi ruoli e responsabilità.
- Assicurare una capacità di risposta efficace agli incidenti di sicurezza, contenendo i tempi di rilevamento, trattamento e ripristino per preservare la continuità del servizio di monitoraggio, secondo le modalità previste dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni*.
- Promuovere il miglioramento continuo del SGSI attraverso audit interni, riesami della direzione, analisi sistematica degli incidenti e valutazioni periodiche dei rischi e delle opportunità.

La misurazione e il monitoraggio del grado di raggiungimento di tali obiettivi sono disciplinati nella *PRO Procedura delle misurazioni e del monitoraggio*, i cui esiti alimentano il riesame della direzione descritto nella *PRO Gestione riesame della direzione*.

6.3 Comunicazione e diffusione della politica

L'organizzazione si adopera per rendere la presente politica comprensibile e accessibile a chiunque ne sia destinatario. All'interno dell'azienda, il documento e i relativi aggiornamenti sono diffusi attraverso i canali aziendali approvati: posta elettronica aziendale, piattaforma documentale del SGSI, strumenti di collaborazione e sessioni di formazione.

L'utilizzo di canali personali non aziendali per la distribuzione di documenti del SGSI non è consentito. Ogni nuova revisione attiva un ciclo di comunicazione coordinato dal **RGQ** , affinché tutto il personale prenda piena consapevolezza dei contenuti e degli impegni espressi.

Nei confronti delle parti interessate esterne, la politica è resa liberamente disponibile attraverso la pubblicazione sul sito web istituzionale di Displaid e, ove opportuno, attraverso il richiamo nei contratti con clienti e fornitori. L'organizzazione promuove la trasparenza dei propri impegni di sicurezza come elemento qualificante della propria offerta di valore verso i committenti del settore delle infrastrutture.

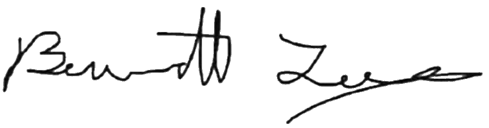
7. Archiviazione e aggiornamento

La presente politica è conservata in formato digitale nel sistema di gestione documentale del SGSI e resa accessibile al personale autorizzato attraverso la piattaforma documentale aziendale. Il **Responsabile del Sistema di Gestione** ne verifica l'adeguatezza almeno una volta all'anno, in occasione del riesame della direzione, o a seguito di significativi mutamenti del contesto organizzativo, del quadro normativo o del panorama delle minacce. Ogni aggiornamento è sottoposto all'approvazione dell' **AD** ; il **RGQ** provvede quindi alla distribuzione della nuova versione attraverso i canali autorizzati, al ritiro delle copie superate e alla loro conservazione nell'archivio storico a garanzia della tracciabilità delle revisioni.

8. Documenti di riferimento

- PRO Processi direzionali
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura delle misurazioni e del monitoraggio
- PRO Gestione riesame della direzione
- PRO Politica di sicurezza delle informazioni

Milano, 8 giugno 2026



MAIL info@displaid.it TEL +39 331 3305637 WEBSITE www.displaid.it Displaid