Displaid

MOD 520

Information Management System Policy

DISPLAID S.R.L. SOCIETÀ BENEFIT
VIA CARLO FREGUGLIA, 2 20122 MILANO
VAT NO: 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

Document version history

VERSION	DATE	AUTHOR	APPROVED BY
1	08/06/2026	Francesco Morgan Bono	Lorenzo Benedetti

DISPLAID S.R.L. SOCIETÀ BENEFIT
VIA CARLO FREGUGLIA, 2 20122 MILANO
VAT NO: 12832220961

Information Management System Policy

1. Purpose

Displaid S.r.l. Società Benefit recognizes the protection of information as an essential prerequisite for pursuing its mission in the field of structural monitoring of critical infrastructure. The organization's activities, which include the design of proprietary IoT hardware, the development of AI-based diagnostic algorithms and the delivery of the monitoring service through the Iris platform, generate, process and store data whose confidentiality, integrity and availability are decisive both for the safety of the monitored structures and for the trust of public and private clients.

This policy expresses Top Management's intention to protect the company's information assets and to steer the Information Security Management System (ISMS) towards objectives consistent with Displaid's operating context, business model and strategic direction. The document provides the framework for setting and reviewing information security objectives, formalizes the commitment to satisfy applicable requirements and promotes the continual improvement of the effectiveness of the ISMS, in keeping with the organization's status as a Società Benefit (benefit corporation) and with the responsibility it feels towards its interested parties.

2. Scope

This policy applies to all activities, processes, information assets and technology systems of Displaid S.r.l. Società Benefit, with reference to the registered office at Via Carlo Freguglia 2, 20122 Milan (MI) and the operational site at Via Colico 36, 20158 Milan (MI). The document is addressed to all employees, collaborators, consultants, contractors and third parties who access company information or systems, regardless of their place of work. The scope covers the entire cycle of design, development, installation and delivery of structural monitoring systems and the associated data analysis services, as well as the supporting administrative and management activities.

3. Normative references

- ISO/IEC 27001:2022
- ISO/IEC 27000:2018
- Regulation (UE) 2016/679
- Italian Legislative Decree 196/2003

4. Terms and definitions

- **Information security:** preservation of confidentiality, integrity and availability of information.
- **Information security management system:** part of the overall management system, based on a risk-based approach, aimed at establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security.
- **Policy:** intentions and direction of an organization, as formally expressed by its Top Management.
- **Interested party:** person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.
- **Continual improvement:** recurring activity to enhance performance.

5. Roles and responsibility

- **AD:** establishes, approves and keeps this policy up to date, ensuring its consistency with the organizational context and the strategic direction of the company.
- **Management System Manager:** supports the **AD** in drafting the policy, verifies its alignment with the context analysis and risk assessment, and coordinates the implementation of information security commitments.
- **RGQ:** is responsible for the formalization, revision control and distribution of the policy to staff and interested parties through authorized company channels.
- **DS:** contributes to defining the strategic direction that guides the policy and promotes its application in institutional and commercial relationships.
- **RDP Production:** ensures that the principles set out in the policy are integrated into the production and delivery processes of the monitoring systems.
- **RDP Support:** ensures that security commitments are applied in technical support, field installation and maintenance activities.
- **RDP Administration:** verifies compliance with information security requirements in administrative and contractual processes and in the management of supplier relationships.

6. Management system commitment and objectives

6.1 Top Management commitment

Displaid's Top Management, aware of the strategic value of information security for a deep-tech company engaged in monitoring bridges, viaducts and critical infrastructure, makes binding commitments through this policy to protect the company's information assets.

The organization promotes a security culture founded on shared responsibility, in which every person who interacts with company data and systems is aware of their role in protecting information. The **AD** allocates the financial, human and technological resources needed to support the ISMS and to integrate security requirements into every process: from the design of the Smart Sensors and diagnostic algorithms to the delivery of the monitoring service through the Iris platform, through to administrative activities and relationships with third parties. The operational arrangements through which Top Management exercises leadership and governance of the ISMS are detailed in the *PRO Processi direzionali*.

Displaid adopts a systematic, risk-oriented approach in which security decisions are proportionate to the assessed level of risk and residual risk is kept within the acceptance threshold defined by the organization. The methods for identifying, assessing and treating risks are described in the *PRO Procedura gestione dei rischi*, whose results feed into the setting of priorities and protection measures.

The company is committed to satisfying applicable legal, regulatory and contractual requirements, with particular attention to the protection of personal data and to the obligations arising from relationships with public-sector clients. Compliance with current legislation and with the commitments made to clients, suppliers, investors and supervisory authorities is an essential condition for the sustainability and credibility of the organization's business model. The fundamental security principles that guide all operational policies and procedures are defined in the *POL Politica di sicurezza delle informazioni.*

The pursuit of continual improvement runs through the entire ISMS: through incident analysis, periodic risk assessments, internal audits and management reviews, Displaid constantly identifies opportunities to strengthen its controls and increase the effectiveness of the protection measures in place.

6.2 Information security objectives

This document provides the framework for setting, reviewing and updating information security objectives. The organization pursues the following strategic objectives, consistent with its context and with Top Management's direction:

- Protect the confidentiality, integrity and availability of the telemetry data acquired by the Smart Sensors, of the proprietary diagnostic algorithms and of all information processed through the Iris platform and the cloud infrastructure.
- Keep residual risk within an acceptable level, applying treatment measures proportionate to the criticality of the assets and to the organization's operating context.
- Satisfy applicable legal, regulatory and contractual requirements, with specific regard to the protection of personal data and to obligations towards public-sector clients.
- Strengthen information security awareness among all staff, through training and awareness programs suited to the different roles and responsibilities.
- Ensure an effective response capability for security incidents, keeping detection, handling and recovery times short in order to preserve the continuity of the monitoring service, as set out in the *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni*.
- Promote the continual improvement of the ISMS through internal audits, management reviews, systematic incident analysis and periodic assessments of risks and opportunities.

The measurement and monitoring of the extent to which these objectives are achieved are governed by the *PRO Procedura delle misurazioni e del monitoraggio*, whose results feed into the management review described in the *PRO Gestione riesame della direzione*.

6.3 Communication and dissemination of the policy

The organization strives to make this policy understandable and accessible to all those to whom it is addressed. Within the company, the document and its updates are disseminated through approved company channels: company email, the ISMS document platform, collaboration tools and training sessions.

The use of personal, non-company channels to distribute ISMS documents is not permitted. Each new revision triggers a communication cycle coordinated by the **RGQ**, so that all staff become fully aware of the content and the commitments expressed.

With regard to external interested parties, the policy is made freely available through publication on Displaid's corporate website and, where appropriate, through reference in contracts with clients and suppliers. The organization promotes transparency of its security commitments as a distinguishing element of its value proposition to clients in the infrastructure sector.

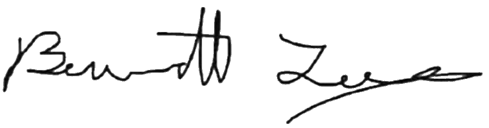
7. Storage and updating

This policy is stored in digital format in the ISMS document management system and made accessible to authorized staff through the company document platform. The **Management System Manager** verifies its adequacy at least once a year, during the management review, or following significant changes in the organizational context, the regulatory framework or the threat landscape. Each update is subject to approval by the **AD**; the **RGQ** then distributes the new version through the authorized channels, withdraws superseded copies and retains them in the historical archive to ensure traceability of revisions.

8. Reference documents

- *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*

Milan, 8 giugno 2026



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