Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

Information Security Policy

Classification: Public

Version	Date	Authors	Changes
0.5	2026/07/10	Nuno Cravino	First Draft
1.0	2026/07/24	Nuno Cravino	First Version

Table of Contents

1. Introduction and Purpose

2. Scope of Application

3. Legal Framework

4. Information Security Principles

    4.1. Confidentiality

    4.2. Integrity

    4.3. Availability

    4.4. Accountability

    4.5. Proportionality

    4.6. Defense in Depth

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

- 4.7. Continuous Improvement
- 4.8. Data Classification

5. Governance and Responsibilities
- 5.1. Management Body
- 5.2. Cybersecurity Officer
- 5.3. Single Point of Contact
- 5.4. Cybersecurity Team
- 5.5. All Network Members

6. Cybersecurity Risk Management
- 6.1. Methodology
- 6.2. Assessment Criteria
- 6.3. Periodicity

7. Cybersecurity Measures
- 7.1. Incident Handling
- 7.2. Business Continuity
- 7.3. Supply Chain Security
- 7.4. Secure Development and Maintenance
- 7.5. Effectiveness Assessment
- 7.6. Training and Cyber Hygiene
- 7.7. Cybersecurity Exercises
- 7.8. Encryption and Access Control
- 7.9. Human Resources Security and Access Control
- 7.10. Authentication and Secure Communications

8. Incident Management
- 8.1. Incident Classification
- 8.2. Response Process
- 8.3. Notification Obligations

9. Business Continuity

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

- 9.1. Business Impact Analysis
- 9.2. Business Continuity and Disaster Recovery Plans
- 9.3. Backup Policy

10. Supply Chain Security
- 10.1. Supplier Inventory
- 10.2. Supplier Assessment
- 10.3. Contractual Requirements

11. Compliance and Auditing
- 11.1. Internal Audits
- 11.2. Technical Testing
- 11.3. Performance Indicators
- 11.4. Reporting to CNCS

12. Violations and Sanctions
- 12.1. Internal Consequences
- 12.2. Legal Sanctions

13. Review and Update
- 13.1. Annual Review
- 13.2. Extraordinary Review
- 13.3. Approval Process

14. Annexes
- Annex A: Glossary
- Annex B: Related Documents

15. Document Approval

---

1. Introduction and Purpose

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

This Information Security Policy establishes the principles, guidelines, and responsibilities for protecting DareData's information assets and those of our clients —both critical and non-critical— in compliance with Decree-Law No. 125/2025, which transposes Directive (EU) 2022/2555 (NIS2) into Portuguese law.

As a consulting and product company serving entities across essential and important sectors, our primary objective is to ensure the confidentiality, integrity, and availability of information, protecting our organization and our clients against cybersecurity threats and incidents.

This policy is the highest-level reference document on cybersecurity matters and must be read in conjunction with the procedures, plans, and work instructions that complement it. All subordinate documents must be consistent with the principles established herein.

---

2. Scope of Application

This policy applies to:

- **Personnel – employees, directors,officers and board members.**
- **External Personnel** – contractors, freelancers, and consultants engaged under service agreements.
- **Third Parties** – suppliers, service providers and business partners with access to the organization's or its clients' systems, code, or data
- All information systems, networks, devices, and data processed or handled by the organization
- Physical and logical infrastructures supporting service provision
- Data processing in cloud, on-premises, and hybrid environments

The policy covers all countries and locations where the organization operates, regardless of local jurisdiction, without prejudice to more stringent legal requirements that may apply locally.

2.1 Definitions

For the purposes of this Policy:

- Personnel – Employees, directors and officers employed directly by DareData.
- Board Members - Individuals who might not be directly employed but have access to internal, confidential and restricted information.
- External Personnel – Individuals engaged by DareData under independent service agreements (including contractors, freelancers and consultants) who are granted access to DareData's or its clients' information, systems or facilities solely for the

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

performance of contracted services. Nothing in this Policy shall be interpreted as creating an employment relationship or a relationship of subordination.
- Third Parties – Suppliers, vendors, partners and other organizations that provide products or services to DareData and may have access to information, systems or facilities under contractual arrangements.

Their work includes:

- Product development, research, and delivery
- Management, administrative, and operational tasks
- Internal consulting, research, and development
- Maintenance and deployment of internal infrastructure, systems, and networks
- Consulting or outsourcing projects for DareData's clients

---

3. Legal Framework

This policy is framed within the following regulatory context, without prejudice to other applicable legal and regulatory obligations:

- Decree-Law No. 125/2025 — transposition of Directive (EU) 2022/2555 (NIS2) for Portugal
- General Data Protection Regulation (GDPR) — Regulation (EU) 2016/679
- Cybercrime Law — Law No. 109/2009, of September 15
- Legal Regime for Cyberspace Security — Law No. 46/2018, of August 13
- ISO/IEC 27001:2022 — Information Security Management System (technical reference)
- National Cybersecurity Reference Framework (QNRCS)
- Technical standards and guidelines issued by the National Cybersecurity Center (CNCS)

In case of conflict between this policy and applicable legal or regulatory provisions, the legal framework prevails. The organization must ensure simultaneous compliance with all applicable regulations.

---

4. Information Security Principles

The organization guides its approach to information security based on the following fundamental principles, which must inform all decisions and actions related to cybersecurity.

4.1. Confidentiality

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

Information must be accessible only to authorized individuals and systems, ensuring that sensitive data is not disclosed to unauthorized parties, whether through deliberate action or accident. Access must be granted based on the principle of least privilege, assigning only the permissions strictly necessary for the performance of duties.

4.2. Integrity

Information must be accurate, complete, and protected against unauthorized or accidental modifications throughout its lifecycle. Integrity control mechanisms must ensure that any unauthorized modification is detected promptly and reported.

4.3. Availability

Systems and information must be available when needed, complying with business continuity requirements and defined service levels.

4.4. Accountability

All actions related to information systems must be traceable to the respective user or process through robust logging, monitoring, and auditing mechanisms. Individual accountability is a necessary condition for the effective operation of security controls.

4.5. Proportionality

Security measures must be proportional to the identified risks, considering the state of the art, implementation costs, the size of the organization, and the nature of the services provided. A risk-based approach allows focusing resources where the potential impact is greatest.

4.6. Defense in Depth

The organization applies multiple layers of security controls so that the failure of one control does not compromise overall security. This approach reduces the attack surface and limits the impact of potential incidents.

4.7. Continuous Improvement

Information security is a continuous process of assessment, learning, and improvement. The organization periodically reviews its security measures in light of the evolving threat landscape and incorporates lessons learned from incidents and exercises.

4.8. Data Classification

The organization classifies its information assets and those of its clients —both critical and non-critical— based on their sensitivity, value, and criticality to ensure appropriate protection measures are applied. Classification considers both internal information and

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

client data handled during consulting or product-related engagements. **Every time a new document is created, the type of classification should be written on the header.**

The classification levels are as follows:

- **Public**: Information that can be freely disclosed without risk to the organization or its clients. Examples include public marketing materials, general corporate information, non-sensitive case studies, and public service descriptions.
- **Internal**: Information intended for internal use. Its unauthorized disclosure could cause minor operational inconvenience or reputational impact. Examples include internal memos, meeting minutes, standard operating procedures, and non-sensitive project documentation. **This is the default level when a document has no other explicit classification.**
- **Confidential**: Information that requires protection due to its sensitivity. Unauthorized access or disclosure could cause significant harm to the organization or its clients, including financial loss, legal liability, or reputational damage. Examples include business strategies, non-public financial data, internal audit reports, trade secrets, intellectual property, client project documentation, personal data whose unauthorized disclosure could adversely affect data subjects or breach applicable data protection legislation , authentication credentials, security configurations, and critical infrastructure details.
    - Access: Restricted to authorized personnel with a need-to-know or designated roles
    - Storage: Encrypted at rest with strong algorithms; protected by access controls
    - Transmission: Encrypted in transit
    - Handling: Logged and monitored
- **Restricted**: Information subject to legal, regulatory, or contractual restrictions, where disclosure is prohibited by law or agreement. Examples include classified government data, legally privileged communications, data protected by non-disclosure agreements (NDAs), special categories of personal data under Article 9 GDPR, and sensitive client data for critical sector entities.
    - Access: Granted only to individuals with specific legal or contractual authorization
    - Storage: Isolated in dedicated, access-controlled systems; encrypted with separately managed keys
    - Transmission: Only through channels explicitly approved for restricted data
    - Handling: Subject to additional logging, monitoring, and audit requirements

Client data must be classified according to the most restrictive requirement between the organization's classification and the client's own classification requirements.

This classification must be reviewed periodically, particularly when the sensitivity or value of the information changes. All network members are responsible for handling

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

information according to its classification level and reporting any suspected misclassification or unauthorized access.

4.9 Shared Responsibility

Information security is a shared responsibility between DareData, its Personnel, External Personnel, Third Parties, and, where applicable, its clients.

Each party is responsible for implementing and maintaining appropriate security measures within the scope of its own systems, assets, services, and contractual obligations.

When Personnel or External Personnel access, develop, administer, or otherwise interact with client-managed systems, infrastructure, applications, or data, they shall comply with:

- this Information Security Policy;
- applicable contractual obligations;
- and any customer-specific security requirements communicated by the client, provided they do not conflict with applicable laws or mandatory internal security requirements.

Where multiple security requirements apply, the more restrictive requirement shall prevail unless otherwise agreed in writing.

Effective information security relies on cooperation, timely communication, and the clear allocation of responsibilities between all parties involved.

DareData remains responsible for the security of its own internal information systems, platforms, products, and managed services, while clients remain responsible for the security of their own environments unless otherwise contractually agreed.

---

5. Governance and Responsibilities

The organization's cybersecurity governance structure ensures clear assignment of responsibilities.

5.1. Management Body

The management body is responsible for approving cybersecurity risk management measures and supervising their execution. Members of the management body must attend regular cybersecurity training and are personally responsible for compliance with legal obligations.

Responsibilities:

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

- Approve this policy and associated security measures
- Allocate adequate human, financial, and technological resources for implementation
- Supervise compliance with the requirements of Decree-Law No. 125/2025
- Attend training on cybersecurity risk management (mandatory by law)
- Approve the incident response plan and business continuity plan
- Review the effectiveness of implemented security measures annually

5.2. Cybersecurity Officer

Rui Figueiredo, managing partner, is designated as the Cybersecurity Officer, under Article 31 of Decree-Law No. 125/2025, with the following functions:

- Implement, maintain, and review the Information Security Policy
- Coordinate cybersecurity risk management and periodic risk assessments
- Manage and coordinate the response to cybersecurity incidents
- Ensure compliance with all applicable regulatory requirements
- Report periodically to the management body on the state of cybersecurity
- Coordinate training, awareness programs, and cybersecurity exercises
- Monitor the threat landscape and adapt measures accordingly

5.3. Single Point of Contact

Rui Figueiredo, managing partner, is designated as the single point of contact with the National Cybersecurity Center (CNCS), under Decree-Law No. 125/2025. The point of contact ensures two-way communication with the competent authorities, including incident notification and the receipt of alerts and guidance.

5.4. Cybersecurity Team

The Cybersecurity Team is responsible for the day-to-day implementation and operational aspects of the organization's cybersecurity program.

Responsibilities:

- Implement and maintain security controls and measures
- Monitor security systems and respond to alerts
- Conduct regular vulnerability assessments and security testing
- Investigate and respond to security incidents
- Maintain security documentation and records
- Provide technical guidance on cybersecurity matters
- Support the Cybersecurity Officer in policy implementation
- Manage security tools and technologies
- Coordinate with the product team on security-related issues
- Coordinate on security-related infrastructure changes

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

5.5. Personnel and External Personnel

Personnel and External Personnel shall comply with the information security requirements applicable to the activities they perform and to the level of access granted to them.

Unless otherwise defined by law, contract, or customer-specific requirements, they are expected to:

- Read, understand and comply with this Information Security Policy and all applicable security procedures.
- Participate in cybersecurity awareness activities and training, where required by their role or contractual obligations.
- Immediately report cybersecurity incidents, anomalies, or suspected security events to the Cybersecurity Team
- Protect authentication credentials and never share them with unauthorized individuals.
- Cooperate, where applicable, with cybersecurity audits, security reviews, and incident investigations.
- Use information systems, devices, and information assets only for authorized business purposes.
- Lock workstation or laptop screens when left unattended.
- Maintain an appropriate separation between personal and professional information and systems, in accordance with the organization's acceptable use requirements.
- Protect the confidentiality of information during and after the termination of their employment or contractual relationship.
- Develop, maintain, or modify software in accordance with the organization's Secure Development Policy and Security by Design principles, where applicable.

5.6 Third Parties

Third Parties shall comply with the information security obligations established in their contractual agreements with DareData. Where Third Parties are granted access to DareData's or its clients' information, systems, or facilities, they shall implement security measures appropriate to the nature of the services provided and cooperate with DareData on cybersecurity matters where contractually agreed.

---

6. Cybersecurity Risk Management

The organization adopts a risk-based approach to cybersecurity management. Risk management is a continuous process supporting security decisions.

6.1. Methodology

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

Risk assessment follows a simple, documented process:

- Identify and inventory critical information assets
- Identify relevant threats and vulnerabilities
- Assess likelihood and impact of each risk
- Define treatment strategies: mitigate, accept, transfer, or avoid
- Implement and monitor selected measures
- Review periodically and update the risk register

6.2. Assessment Criteria

Risk assessment considers:

- The organization's exposure to risks and known threats
- Probability and severity of incidents
- Impact on clients, especially critical sector entities
- Cost-effectiveness of risk management measures
- The size and nature of the organization

6.3. Periodicity

Risk assessment is conducted at least once a year and updated when significant changes occur, such as:

- Major changes in infrastructure or systems
- Introduction of new services or processes
- Identification of new high-impact threats
- Serious cybersecurity incidents
- Changes in applicable regulations

---

7. Cybersecurity Measures

The organization implements essential cybersecurity measures proportional to identified risks.

7.1. Incident Handling

Documented procedures exist for detecting, classifying, containing, and recovering from cybersecurity incidents. Incident handling details are in the Incident Response Plan. All incidents are recorded for analysis and improvement.

7.2. Business Continuity

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

A Business Continuity Plan ensures critical operations can continue during disruptions. Backups are stored separately and tested regularly.

7.3. Third-Party and Supply Chain Security

The organization manages cybersecurity risks arising from its supply chain through a risk-based approach covering technology providers, external service providers, contractors, and business partners.

Prior to onboarding, and periodically thereafter where appropriate, suppliers and service providers shall be assessed according to the nature of the services provided, the level of access granted to information or systems, and the potential impact on the organization's operations and its clients.

Security requirements shall be established through contractual, legal, or regulatory obligations, as appropriate, and may include:

- confidentiality obligations;
- information security requirements;
- incident notification obligations;
- access control requirements;
- data protection obligations;
- compliance with applicable laws and contractual commitments;
- right to request evidence of security controls, where contractually agreed.

The organization shall maintain an inventory of suppliers and service providers with access to information, systems, or client data and periodically review the associated cybersecurity risks.

Where suppliers, contractors, or business partners are granted access to client-managed environments, they shall also comply with the applicable customer security requirements communicated by DareData or the client, where contractually applicable.

7.4. Customer Managed Environments

DareData personnel and External Personnel may perform activities within customer-managed environments, including information systems, cloud platforms, development environments, networks, repositories, and devices.

When accessing or operating within customer-managed environments, the following principles shall apply:

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

- access shall be granted only when authorized and limited to the minimum privileges required for the assigned activities;
- customer information, assets, and systems shall be used solely for authorized business purposes;
- customer-specific security requirements, policies, and procedures shall be complied with, where contractually applicable;
- authentication credentials provided by customers shall be protected and shall not be shared;
- security incidents affecting customer-managed environments shall be reported without undue delay, in accordance with contractual obligations and DareData's Incident Management process;
- any data obtained from customer-managed environments shall be handled in accordance with applicable contractual, legal, and regulatory requirements.

Where both DareData and customer security requirements apply, the more restrictive requirement shall prevail unless otherwise agreed in writing.

7.5. Secure Development and Maintenance

The organization adopts secure development and maintenance practices throughout the software development lifecycle to reduce cybersecurity risks and improve the resilience of its products and services.

Secure development activities shall include, where applicable:

- secure-by-design and security-by-default principles;
- security requirements during solution design;
- secure coding practices;
- peer review or pull request review before deployment;
- protection of source code repositories;
- secure management of secrets, credentials, and cryptographic keys;
- management of third-party libraries and software dependencies;
- vulnerability identification and remediation throughout the development lifecycle;
- testing appropriate to the risks associated with the solution;
- change management procedures for production deployments.

Where artificial intelligence tools are used to assist software development, generated outputs shall be reviewed and validated by qualified personnel before deployment into production.

Development, testing, and production environments shall be appropriately segregated whenever feasible.

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

7.6 Responsible Use of Artificial Intelligence

The organization recognizes the benefits of Artificial Intelligence (AI) technologies while ensuring that their use does not compromise information security, confidentiality, privacy, intellectual property, or legal and contractual obligations.

- Personnel and External Personnel using AI tools as part of their professional activities shall:
- use only AI services that have been approved or authorized by the organization, where required;
- avoid submitting confidential information, personal data, source code, customer information, authentication credentials, or other sensitive information to public AI services unless expressly authorized and appropriate safeguards are in place;
- verify and validate AI-generated outputs before using them in business decisions, software development, customer deliverables, or production environments;
- respect applicable intellectual property, copyright, confidentiality, and data protection obligations when using AI tools;
- ensure that AI is used to support, and not replace, professional judgement where human oversight is required;
- comply with customer-specific restrictions regarding the use of AI technologies where contractually applicable.

The organization may establish additional procedures governing the selection, approval, monitoring, and acceptable use of AI technologies.

The use of Artificial Intelligence shall follow the principles of transparency, accountability, human oversight, security, and compliance with applicable legal, regulatory, and contractual requirements.

7.7. Effectiveness Assessment

The organization tracks cybersecurity KPIs and conducts periodic internal audits to assess measure effectiveness.

7.8. Training and Cyber Hygiene

The organization shall ensure that Personnel and, where applicable, External Personnel receive information security and cybersecurity awareness training appropriate to their roles and responsibilities.

- Training shall be provided:
- during onboarding;
- periodically thereafter, at least annually;
- following significant changes to the organization's security policies, technologies, or threat landscape;
- when personnel change roles and assume new security responsibilities.

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

The organization may conduct awareness campaigns, phishing simulations, and other activities to promote a strong cybersecurity culture.

7.9. Cybersecurity Exercises

Periodic simulations, including phishing tests and tabletop exercises, are conducted to improve procedures, response, and awareness.

7.10. Encryption and Access Control

Data in transit and at rest is encrypted. Access follows the principle of least privilege, with MFA required for critical systems and remote access. Access is reviewed regularly and deactivated when no longer needed.

7.11. Human Resources Security and Access Control

The organization applies the principle of least privilege in access management, ensuring that each user has only the permissions necessary for their role. Multi-Factor Authentication (MFA) is mandatory for access to critical systems and remote access.

Where legally permissible and proportionate to the nature of the role, pre-employment screening or background verification may be performed in accordance with applicable laws and regulations.

Access rights shall be reviewed whenever personnel change roles or responsibilities and shall be revoked promptly upon the termination or completion of the employment or contractual relationship.

Privileged access shall be subject to periodic review, at least quarterly.

Personnel and External Personnel shall remain bound by applicable confidentiality obligations after the termination of their employment or contractual relationship, where required by law, contract, or confidentiality agreements.

7.12. Authentication and Secure Communications

The organization implements robust authentication mechanisms, with mandatory MFA for high-criticality systems. Communications between systems and with external parties are protected by up-to-date cryptographic protocols.

Network segmentation and traffic monitoring allow detection of unauthorized access and anomalous behavior. Remote access to sensitive systems is performed exclusively through VPN connections with strong authentication.

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

8. Incident Management

The organization has a structured process for managing cybersecurity incidents, detailed in the Incident Response Plan.

8.1. Incident Classification

Incidents are classified by severity: low, medium, high, or critical. Classification determines response procedures and communication requirements.

8.2. Response Process

The process includes: detection, containment, eradication, recovery, and post-incident analysis with lessons learned.

8.3. Notification Obligations

Significant incidents are reported to CNCS within: 24 hours (early warning), 72 hours (initial notification), and 30 days (final report). All incidents are internally recorded.

---

9. Business Continuity

The organization maintains a Business Continuity Plan to ensure critical operations can continue during disruptions.

9.1. Business Impact Analysis

Identifies critical processes, minimum resource requirements, and recovery objectives (RTO and RPO).

9.2. Business Continuity and Disaster Recovery Plans

Document procedures for maintaining operations during interruptions and restoring systems after major failures. Plans are tested at least annually.

9.3. Backup Policy

Backups are stored separately, tested regularly, and retained according to business needs.

9.4. Crisis Management Structure

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

A named crisis management team, roles and decision-making authority during a disruption, escalation criteria (when does an incident become a "crisis"), and internal/external communication plan (staff, clients, authorities).

9.4. Testing Regime

Tabletop exercises and full failover tests are conducted at defined intervals, with results documented and identified gaps remediated within a defined timeframe.

---

10. Supply Chain Security

The organization manages risks from suppliers and service providers.

10.1. Supplier Inventory

Maintains an updated list of suppliers with access to systems or data, including their criticality level.

10.2. Supplier Assessment

Assesses supplier cybersecurity practices before onboarding and periodically thereafter.

10.3. Contractual Requirements

Contracts with critical suppliers include security clauses, incident notification obligations, and audit rights.

---

11. Compliance and Auditing

The organization verifies compliance through regular checks.

11.1. Internal Audits

The organization shall establish and maintain a risk-based internal audit programme to evaluate the effectiveness of the Information Security Management System (ISMS), compliance with this Policy, and the implementation of applicable security controls.

Internal audits shall be planned considering the significance of the processes, identified risks, previous audit results, and organizational changes, ensuring that all relevant areas of the ISMS are periodically reviewed.

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

11.2. Technical Testing

Technical security testing, including vulnerability assessments and penetration testing where appropriate, shall be performed periodically based on risk, significant changes to the environment, and applicable legal, regulatory, or contractual requirements.

Identified vulnerabilities shall be assessed, prioritized, and remediated in accordance with the organization's Vulnerability Management process.

11.3. Performance Indicators

The organization shall define, monitor, and periodically review information security performance indicators to evaluate the effectiveness of the Information Security Management System and support continual improvement.

- Performance indicators may include, where applicable:
- completion of security awareness training;
- phishing simulation results;
- security incidents and response times;
- vulnerability remediation performance;
- privileged access reviews;
- audit findings and corrective actions;
- information security risks and treatment status;
- compliance with security policies and procedures.

11.4. Reporting to CNCS

The organization will report to CNCS as required by law, providing information on implemented cybersecurity measures.

---

12. Violations and Sanctions

Non-compliance with this policy may result in disciplinary action and legal consequences.

12.1. Internal Consequences

Violations may result in additional training, formal warnings, suspension, or termination, depending on severity.

12.2. Legal Sanctions

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

Non-compliance with Decree-Law No. 125/2025 may result in fines up to €10,000,000 or 2% of annual turnover for essential entities, and up to €7,000,000 or 1.4% for important entities.

12.3. Security Exceptions

Any exception to the requirements established in this Policy shall be formally documented, justified, risk-assessed, and approved by the appropriate management authority prior to implementation, unless an emergency situation requires immediate action.

Approved exceptions shall be periodically reviewed and withdrawn when no longer justified.

---

13. Review and Update

This policy is reviewed and updated regularly to remain effective.

13.1. Annual Review

The policy is reviewed at least once a year.

13.2. Extraordinary Review

The policy is also reviewed when significant changes occur, such as major incidents, structural changes, or regulatory updates.

13.3. Approval Process

Changes are proposed by the Cybersecurity Officer, reviewed by the cybersecurity team, and approved by management. The updated version is communicated to all Network Members.

---

14. Annexes

Annex A: Glossary

The terms used in this policy have the following meanings:

- **The Organization** — DareData SA
- **CNCS** — National Cybersecurity Center: The national authority responsible for cybersecurity in Portugal

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

- **CSIRT** — Computer Security Incident Response Team: Cybersecurity incident response team
- **Decree-Law No. 125/2025** — The diploma transposing the NIS2 Directive into Portuguese law
- **NIS2** — Directive (EU) 2022/2555: The second EU directive on high-level cybersecurity measures across the Union
- **Essential entity** — An entity providing services in highly critical sectors (Annex I of Decree-Law No. 125/2025)
- **Important entity** — An entity providing services in other critical sectors (Annex II of Decree-Law No. 125/2025)
- **Significant incident** — An incident with considerable impact on service provision, according to the criteria of Article 39 of Decree-Law No. 125/2025
- **MFA** — Multi-Factor Authentication: An authentication method requiring two or more verification factors
- **VPN** — Virtual Private Network: Technology that creates a secure, encrypted connection over insecure networks
- **RTO** — Recovery Time Objective: The maximum tolerable time to restore a service after an interruption
- **RPO** — Recovery Point Objective: The maximum tolerable data loss, measured in time
- **BIA** — Business Impact Analysis: An assessment of the consequences of interrupting critical processes
- **BCP** — Business Continuity Plan: A document defining how to maintain operations during an interruption
- **DRP** — Disaster Recovery Plan: A document defining how to restore systems after a serious failure
- **Phishing** — A social engineering technique used to obtain credentials or sensitive information through fraudulent communications

Annex B: Related Documents

This policy must be read in conjunction with the following documents, which complement and detail it:

- **Cybersecurity Incident Response Plan – Confidencial**
- **Access and Identity Management Policy – Internal**
- **Remote Work and Mobile Devices Policy – Internal**

---

15. Document Approval

Docusign Envelope ID: B44989A6-F30E-8398-8109-7296F9FA714C

Role	Name	Position	Date and Signature	
Prepared by	Nuno Cravino	Cybersecurity Lead	8/20/2026	Assinado por: Nuno Cravino 7D8BDDE8458D421...
Reviewed by	Marta Duarte and Francsico Ruas.	Cybersecurity Team	8/20/2026	DocuSigned by: Marta Duarte C884AC83425E4A9...
Approved by	Rui Figueiredo, Nuno Brás and Ivo Bernardo	Cybersecurity Officer and Adminstration	8/20/2026	Signed by: Rui Figueiredo B7E39E669957452...
Communicated to	Personnel and External Personnel			

This document is controlled by the organization's document management system. Changes require formal approval as per the table above. The next review must occur by 01st, December 2027.