without a doubt

Information Security & Cybersecurity Overview (External)

January 2026

Boltrics

Purpose of this document

This document provides customers, partners and auditors with a high-level, externally shareable overview of how Boltrics addresses information security and cybersecurity risks. It is designed to offer transparency and assurance regarding Boltrics' governance, risk management and security practices without disclosing sensitive internal security details.

The document reflects how Boltrics aligns its approach with the NIS2 Directive and the European Union Agency for Cybersecurity (ENISA) cybersecurity risk-management framework. It does not describe internal technical configurations, nor does it constitute a certification, guarantee or contractual commitment.

Scope & approach

Boltrics develops and delivers SaaS solutions in the logistics domain, primarily operating on Microsoft Azure and Microsoft Dynamics 365 Business Central. Boltrics has established an information- and cybersecurity governance framework that is:

- Risk-based and proportionate to the nature, scale and complexity of its services;
- Aligned with applicable NIS2 obligations and related national legislation;
- Inspired by ENISA guidance and internationally recognized best practices; and
- Continuously reviewed and improved as part of its Information Security Management System (ISMS).

The measures described below explain how Boltrics gives practical effect to these principles. They are presented as guidelines and controls, not as prescriptive technical standards or immutable operating procedures.

Alignment with ENISA / NIS2 requirements

In line with the structure used by ENISA, this document addresses the following technical and methodological areas:

1. Network and information system security policy
2. Risk management
3. Incident handling and response
4. Business continuity and crisis management
5. Supply-chain and third-party security
6. Secure acquisition, development and maintenance of systems
7. Monitoring and evaluation of effectiveness
8. Cyber hygiene and security awareness
9. Cryptography
10. Human-resources security
11. Access control
12. Asset management
13. Physical and environmental security

1. Network and information system security policy

Boltrics maintains a documented Information & Cybersecurity Policy. The policy establishes amongst others:

- Security objectives and guiding principles;
- Roles, responsibilities and escalation paths;
- Governance and oversight structures; and
- Alignment with applicable legal and regulatory requirements, including NIS2.

The policy is reviewed periodically and updated in response to regulatory, technological or organizational changes.

2. Risk management

Boltrics applies a structured, risk-based approach to information security, including:

- Identification and classification of relevant information assets;
- Assessment of threats, vulnerabilities and potential impact;
- Selection of proportionate mitigating measures; and
- Periodic reassessment and management review.

Cybersecurity risks are addressed as part of Boltrics' broader enterprise-risk and supplier-risk management processes.

3. Incident handling and response

Boltrics has established an Incident Response Framework designed to enable timely and coordinated response to security incidents. This framework includes:

- Clearly defined roles, including Cyber Incident Manager, IT Operations and Security Lead;
- Procedures for detection, analysis, containment, remediation and recovery;
- Internal escalation and decision-making mechanisms; and
- Post-incident evaluation and improvement activities.

Where legally required, incidents are assessed for notification obligations towards customers and competent authorities.

4. Business continuity and crisis management

Business continuity and resilience are addressed through:

- Use of Microsoft Azure and Dynamics 365 Business Central availability and resilience controls;
- Backup and recovery mechanisms aligned with service criticality;
- Documented continuity and recovery procedures;
- Backup and recovery measures are periodically tested in line with operational requirements; and
- Defined crisis-management roles and communication lines.

These measures are intended to support timely restoration of availability and access to data following disruptive events.

5. Supply-chain and third-party security

Boltrics recognizes that cybersecurity risks may arise through suppliers and partners. Third-party risks are managed through:

- Contractual security and compliance requirements;
- Risk-based assessment of critical suppliers;
- Reliance on audited cloud-provider controls and certifications (notably Microsoft);
- Periodic review of supplier-related risks relevant to service delivery.

6. Secure acquisition, development and maintenance

Security considerations are embedded throughout the lifecycle of systems and services, including:

- Secure configuration and change-management practices;
- Segregation of development, test and production environments;
- Controlled access to systems and code repositories; and
- Use of Microsoft platform security capabilities.

Security requirements are considered during acquisition, development, maintenance and upgrade activities.

7. Monitoring and evaluation of effectiveness

Boltrics evaluates the effectiveness of its security measures through:

- Management oversight and internal reviews;
- Evaluation of security incidents and near-misses;
- Audit-readiness activities and independent assessments where appropriate; and - Continuous improvement initiatives within the ISMS.

8. Cyber hygiene and security awareness

Boltrics promotes a strong security culture by:

- Implementing baseline cyber-hygiene practices;
- Providing periodic security and compliance awareness training (including privacy, and NIS2-related topics);
- Enforcing confidentiality obligations; and
- Maintaining clear internal security guidance for staff.

9. Cryptography

Cryptographic measures are applied where appropriate, including:

- Encryption of data at rest and in transit;
- Secure key-management practices using Microsoft Azure facilities; and
- Use of industry-standard cryptographic protocols supported by the underlying platforms.

10. Human-resources security

Security responsibilities are embedded in HR processes, including:

- Role-based access principles;
- Confidentiality obligations;
- Security awareness and training; and
- Defined onboarding and offboarding controls.

11. Access control

Access to systems and data is governed by:

- Role-based access control;
- Least-privilege principles;
- Multi-factor authentication for privileged access; and
- Centralised access management and logging.

12. Asset management

Boltrics maintains visibility over relevant information assets by: - Identifying and classifying systems and data; - Assigning ownership and responsibility; and - Aligning protection measures with asset criticality.

13. Physical and environmental security

Physical and environmental security is addressed through:

- Reliance on Microsoft Azure data-centre controls;
- Managed office and workplace security measures; and
- Protection of devices used to access company or customer data.

Relationship with Microsoft

Boltrics' products are built on Microsoft cloud infrastructure and platforms. Microsoft acts as the underlying cloud and platform provider and is solely responsible for the security, availability and compliance of its own cloud and platform products and services, in accordance with the applicable Microsoft agreements.

Boltrics monitors relevant Microsoft certifications, compliance documentation and service assurances as part of its supplier and third-party risk management processes.

In the design and development of 3PL Dynamics and other Boltrics applications, Boltrics applies privacy-by-design and privacy-by-default principles in line with its role as processor, as further described in the applicable Data Processing Agreement.

Disclaimer

This document is provided for general information and assurance purposes only.

- It does not constitute a binding security commitment, certification or warranty.
- It does not replace contractual agreements or legally binding security obligations.
- Descriptions of measures reflect guidelines and practices, not prescriptive technical standards.

- Detailed internal security controls, configurations and procedures are intentionally not disclosed for security reasons.
- Boltrics reserves the right to adapt its security measures in response to evolving risks, technologies, regulatory requirements and business needs.
- For contractual security obligations, reference is made exclusively to the applicable agreements concluded with Boltrics.

Updates and changes

Boltrics may amend or update this document from time to time, including where required or deemed appropriate in light of changes to services, security practices, Microsoft requirements, legal or regulatory obligations, or evolving risk profiles. Updates will be communicated via Boltrics' customary channels.


Boltrics