PRIMA ELECTRO
CUSTOM DESIGNED ELECTRONICS
GROUPE SYNOV

INFORMATION SECURITY & CYBERSECURITY STATEMENT

NIS2 and recognised information-security management principles
For Customer & Prospect Security Evaluations

Classification: C0 - PUBLIC

APPLICATION MATRIX

BU			Site				
x	Prima Electro		Specific (*)		European	x	Global

(*) See the SCOPE OF SITES table on page 2.

Copyright and usage notice

This document is intended to support customer and prospect security evaluations and supply-chain due diligence. It summarizes Prima Electro security governance, enterprise IT controls, operational resilience and third-party security management. It does not replace contracts, non-disclosure agreements, product-specific documentation, formal certifications, independent audit reports or legal advice.
More detailed evidence may be made available according to relevance and confidentiality requirements and, where appropriate, under NDA. Product-specific cybersecurity and product regulatory compliance are outside the scope of this revision.

REVISION MATRIX

Ed.	Rev.	Date	Description	Owner	Class.	Distribution
1	01	14/07/2026	First external issue focused on corporate information security and cybersecurity controls	Digital Innovation & Security	C0 - PUBLIC	Sales / customers / prospects

SCOPE OF SITES

Company	Operational site	Country
Prima Electro	Barone Canavese (TO)	ITALY
Prima Electro	Moncalieri (TO)	ITALY
Prima Electro Suzhou Co. , Ltd	Suzhou	CHINA

(c) 2026 - PRIMA ELECTRO - All rights reserved.

Contents

1. Company Profile and Scope 4
2. Cybersecurity Governance 4
2.1 Leadership and accountability 4
2.2 Information Security Management System and policies 4
2.3 Cyber risk management and regulatory alignment 4
3. Enterprise IT Security 5
3.1 Identity, access control and authentication 5
3.2 Endpoint, network and cloud security 5
3.3 Asset management and information protection 5
3.4 Vulnerability, patch and security monitoring 5
3.5 Awareness, training and personnel security 6
4. Operational Resilience and Incident Management 6
5. Third-Party and Supply Chain Security 6
6. Assurance, Standards and Continuous Improvement 6
6.1 Control assurance and evidence 6
6.2 NIS2 Directive 7
6.3 ISO/IEC 27001 alignment 7
7. Contact and Document Information 7

(c) 2026 - PRIMA ELECTRO - All rights reserved.

1. Company Profile and Scope

Prima Electro S.p.A. designs and manufactures customer-specific electronics and power electronics solutions for selected industrial customers. Prima Electro is part of Groupe Synov and operates through two Italian sites in the Turin area, at Barone Canavese and Moncalieri, together with a production presence in China. The organization supports design, industrialization and serial production activities for complex electronic products and power electronics assemblies.

Prima Electro serves a limited number of selected large multinational customers. Its operating model requires protection of customer information, engineering know-how, business data, manufacturing continuity and controlled supplier relationships throughout the design-to-production lifecycle.

SCOPE	This statement describes the organization and principal measures used by Prima Electro to protect the confidentiality, integrity and availability of company, customer and partner information. It covers corporate IT, relevant operational technology, people, processes, business continuity and third-party security.

2. Cybersecurity Governance

2.1 Leadership and accountability

Prima Electro has established cybersecurity leadership and accountability within its organization. Cybersecurity roles and management responsibilities are formalized as part of the **NIS2 governance programme** and are integrated with business and operational ownership.

- The cybersecurity point of contact and operational leadership are assigned to the CISO and the Infrastructure and Cybersecurity function.
- The Digital Innovation & Security Department coordinates strategic security, information security and related improvement initiatives.
- Responsibilities are distributed across IT, business functions, operations and management according to role and process ownership.
- Governance is reviewed periodically considering business objectives, customer requirements, regulatory obligations and the evolving threat landscape.

2.2 Information Security Management System and policies

Prima Electro operates an Information Security Management System document framework. Policies, procedures and operating instructions address acceptable use, information classification, access management, incident management, backup and continuity, supplier security and related controls.

- Policies and procedures are distributed and made available through the internal ISMS portal.
- Information classification and handling requirements are defined for business information and data.
- Policies and controls are maintained through periodic reviews and compliance checks.

2.3 Cyber risk management and regulatory alignment

Prima Electro is subject to NIS2 as an important entity. The organization maintains a structured programme covering governance, cyber risk management, business continuity, incident response, supply-chain security, technical controls and management oversight.

- Cyber risks are recorded with assigned owners, treatment actions and residual-risk evaluation.
- Risk assessment and business impact analysis activities support prioritization of security and continuity measures.
- Management review and control monitoring support ongoing remediation and continuous improvement.

NIS2 ALIGNMENT	Prima Electro applies a risk-based security governance model aligned with the obligations applicable to important entities, including incident management, continuity, supply-chain security and management accountability.

(c) 2026 - PRIMA ELECTRO - All rights reserved.

3. Enterprise IT Security

3.1 Identity, access control and authentication

Access to information systems is managed through named accounts, structured authorization processes and periodic review of privileges. Access requests are approved according to roles, business need and least-privilege principles.

- Remote access is restricted through VPN technology protected by multi-factor authentication.
- Multi-factor authentication is applied to remote access and to internal and external services according to risk, criticality and technical applicability.
- Access Control Lists are managed according to need-to-know and least privilege principles.
- Privileged access is restricted to authorized IT personnel and authorized third parties.
- Privileged Access Management is implemented for administrator access.
- Administrative operations on endpoints are audited and managed through controlled privilege-elevation and approval mechanisms.

3.2 Endpoint, network and cloud security

Prima Electro applies layered technical security controls across endpoints, networks, cloud and virtualization environments and Internet-facing services. Security architecture includes perimeter protection, segmented networks and controlled access between environments according to resource type and criticality.

- Endpoint and mobile assets are encrypted and managed through the endpoint security suite.
- Patch monitoring and deployment are supported through automated tools for endpoints and servers.
- Vulnerability assessment and penetration testing are performed periodically on exposed information systems, including infrastructure and application layers. Continuous vulnerability assessment capabilities are in place.
- Cloud and virtualization security policies and procedures are documented, approved, communicated, maintained and reviewed at least annually.
- External MDR/XDR services and internal IT availability support emergency response and operational continuity.

3.3 Asset management and information protection

ICT assets are tracked using an asset inventory tool, with maintenance plans and security update policies documented and implemented. Rules for the proper use of company information systems are defined and distributed through the ISMS portal.

- Asset lifecycle procedures are documented for ICT assets, and critical OT assets are identified and inventoried.
- Information classification policies are defined and available for use by business units.
- Digital information and data are protected according to their classification and risk level, including encryption where appropriate. Backup and restoration procedures are periodically verified and include measures such as immutability, encryption at rest and off-site replication.

3.4 Vulnerability, patch and security monitoring

Technical vulnerabilities and security updates are managed through structured monitoring, assessment, testing and deployment processes. Controls are proportionate to system exposure and criticality.

- Automated tools support patch monitoring and deployment for endpoints and servers.
- Vulnerability assessment and penetration testing are performed periodically on exposed infrastructure and application layers.
- Security events are monitored through endpoint, network and managed detection capabilities, with escalation to internal and external specialists where required.

(c) 2026 - PRIMA ELECTRO - All rights reserved.

3.5 Awareness, training and personnel security

Cybersecurity training and awareness activities have been conducted continuously since 2023. Ethical phishing campaigns are performed periodically, with monitored results and specific training suggestions based on campaign outcomes and user roles.

- Security awareness training is continuous and role-aware.
- Phishing simulations are used to identify training needs.
- Role-specific cybersecurity courses are defined based on testing results and job role.
- Cybersecurity courses are documented in a training plan prepared and maintained jointly by ICT and HR. The plan is reviewed periodically.

4. Operational Resilience and Incident Management

Prima Electro maintains governance for information security incidents, crisis management, business continuity and disaster recovery. The objective is to limit operational impact, restore critical services and support timely communication with relevant stakeholders.

- Business continuity priorities are informed by business impact analysis and cyber risk assessment.
- Recovery capabilities are supported by tested backup, restoration and disaster-recovery procedures.
- Security incidents are reported, assessed, escalated and documented according to defined processes.
- Where applicable, notifications are managed in accordance with NIS2, ACN and CSIRT requirements and with contractual stakeholder obligations.
- Internal IT availability and external specialist support contribute to emergency response and operational continuity.

5. Third-Party and Supply Chain Security

Prima Electro recognises supply-chain security as an essential component of information security and NIS2 compliance. Critical suppliers and service providers are identified and assessed through a risk-based process that considers the confidentiality, integrity and availability of the assets and services they provide, together with their potential impact on business continuity.

- Critical suppliers are classified according to the risk and potential impact associated with the supplied service, product or information access.
- Assessment activities consider governance, information security controls, continuity arrangements and relevant physical-security measures.
- Supplier-security verification is maintained over time through onboarding checks, periodic reassessment and follow-up actions where maturity or evidence is limited.
- Contracts include information-security requirements, confidentiality obligations and, where applicable, flow-down of relevant requirements through the supplier chain.
- Infrastructure and technology service providers, including telecommunications, energy and cloud services, are managed through defined service levels and continuity expectations.
- The supplier-security process is updated for new suppliers and material changes to existing services or risk exposure.

6. Assurance, Standards and Continuous Improvement

6.1 Control assurance and evidence

Prima Electro periodically reviews cybersecurity policies, technical controls, risk treatments and supplier requirements. Improvement actions are assigned, monitored and prioritised according to risk and business relevance. Customer questionnaires and reasonable evidence requests are managed through the Digital Innovation & Security Department, subject to confidentiality and need-to-know constraints.

(c) 2026 - PRIMA ELECTRO - All rights reserved.

- This statement is a summary of the corporate security posture and is not an independent audit or certification report.
- Detailed policies, technical evidence or contractual commitments may be provided separately where relevant and authorised.

6.2 NIS2 Directive

Prima Electro is subject to NIS2 as an important entity. The NIS2 programme is used as a driver for governance, risk management, incident reporting, business continuity, supply-chain security and management accountability.

6.3 ISO/IEC 27001 alignment

Prima Electro maintains an ISMS-oriented policy framework and implements controls aligned with recognised information-security management principles. This statement does not claim ISO/IEC 27001 certification unless such certification is separately and formally confirmed by Prima Electro.

Reference	Context
Directive (EU) 2022/2555 - NIS2	Governance, risk management, continuity, incident reporting and supply-chain security
ISO/IEC 27001 principles	Information Security Management System structure and control framework

7. Contact and Document Information

For information-security enquiries, customer or prospect assessments, and requests for additional evidence, please contact:

security@primaelectro.com

This email address has also been shared with all Prima Electro suppliers as the dedicated contact point for promptly reporting information security issues, including security incidents, cyberattacks, compromised email accounts, data breaches, or other events that may affect Prima Electro's information or systems.

(c) 2026 - PRIMA ELECTRO - All rights reserved.