DICHIARAZIONE SULLA SICUREZZA DELLE INFORMAZIONI E CYBERSECURITY

NIS2 e principi riconosciuti di gestione della sicurezza delle informazioni
per le valutazioni di sicurezza di clienti e potenziali clienti (*Prospect*)

Classificazione: C0 - PUBBLICO

MATRICE DI APPLICAZIONE

BU			**Sito**				
x	Prima Electro		Specifico (*)		Europeo	x	Globale

(*) Si veda la tabella PERIMETRO DEI SITI a pagina 2.

Nota sul copyright e sull'utilizzo

Il presente documento ha lo scopo di supportare le valutazioni di sicurezza da parte di clienti e potenziali clienti, nonché la due diligence della catena di fornitura. Esso riassume la governance della sicurezza, i controlli IT aziendali, la resilienza operativa e la gestione della sicurezza delle terze parti di Prima Electro. Non sostituisce contratti, accordi di riservatezza (NDA), documentazione specifica di prodotto, certificazioni formali, relazioni di audit indipendenti o pareri legali.
Evidenze più dettagliate potranno essere rese disponibili in base alla rilevanza e ai requisiti di riservatezza e, ove opportuno, sotto NDA. La cybersecurity specifica di prodotto e la conformità normativa dei prodotti esulano dall'ambito di applicazione della presente revisione.

MATRICE DI REVISIONE

Ed.	Rev.	Data	Descrizione	Owner	Class.	Distribuzione
1	01	14/07/2026	Prima emissione esterna focalizzata sulla sicurezza delle informazioni aziendali e sui controlli di cybersecurity	Digital Innovation & Security	C0 - PUBLIC	Vendite/Clienti/Potenziali clienti

PERIMETRO DEI SITI

Società	Sito operativo	Paese
Prima Electro	Barone Canavese (TO)	ITALIA
Prima Electro	Moncalieri (TO)	ITALIA
Prima Electro Suzhou Co. , Ltd	Suzhou	CINA

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

Contenuti

1. PROFILO AZIENDALE E PERIMETRO DI APPLICAZIONE 4
2. GOVERNANCE DELLA CYBERSECURITY 4
2.1 Leadership e responsabilità 4
2.2 Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e politiche 4
2.3 Gestione del rischio cyber e adeguamento normativo 4
3. SICUREZZA IT AZIENDALE 5
3.1 Identità, controllo degli accessi e autenticazione 5
3.2 Sicurezza degli endpoint, della rete e del cloud 5
3.3 Gestione degli asset e protezione delle informazioni 5
3.4 Monitoraggio delle vulnerabilità, delle patch e della sicurezza 6
3.5 Consapevolezza, formazione e sicurezza del personale 6
4. RESILIENZA OPERATIVA E GESTIONE DEGLI INCIDENTI 6
5. SICUREZZA DELLE TERZE PARTI E DELLA CATENA DI APPROVVIGIONAMENTO (SUPPLY CHAIN) 6
6. GARANZIA DEI CONTROLLI, STANDARD E MIGLIORAMENTO CONTINUO 7
6.1 Garanzia dei controlli ed evidenze 7
6.2 Direttiva NIS2 7
6.3 Allineamento ISO/IEC 27001 7
7. CONTATTI E INFORMAZIONI SUL DOCUMENTO 7

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

1. Profilo aziendale e perimetro di applicazione

Prima Electro S.p.A. progetta e produce soluzioni elettroniche e di elettronica di potenza personalizzate per clienti industriali selezionati. Prima Electro fa parte di Groupe Synov e opera attraverso due siti italiani nell'area di Torino, a Barone Canavese e Moncalieri, insieme a una presenza produttiva in Cina. L'organizzazione supporta le attività di progettazione, industrializzazione e produzione in serie per prodotti elettronici complessi e gruppi di elettronica di potenza.
Prima Electro serve un numero limitato di grandi clienti multinazionali selezionati. Il suo modello operativo richiede la protezione delle informazioni dei clienti, del know-how ingegneristico, dei dati aziendali, della continuità produttiva e delle relazioni controllate con i fornitori lungo l'intero ciclo di vita, dalla progettazione alla produzione.

PERIMETRO	La presente dichiarazione descrive l'organizzazione e le principali misure adottate da Prima Electro per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni aziendali, dei clienti e dei partner. Copre l'IT aziendale, la tecnologia operativa (OT) pertinente, il personale, i processi, la continuità operativa e la sicurezza delle terze parti.

2. Governance della cybersecurity

2.1 Leadership e responsabilità

Prima Electro ha definito ruoli di leadership e responsabilità per la cybersecurity all'interno della propria organizzazione. I ruoli di cybersecurity e le responsabilità di gestione sono formalizzati nell'ambito del **programma di governance NIS2** e sono integrati con la proprietà aziendale e operativa.

- Il punto di contatto per la cybersecurity e la leadership operativa sono affidati al CISO e alla funzione *Infrastructure and Cybersecurity.*
- Il dipartimento Digital Innovation & Security coordina la sicurezza strategica, la sicurezza delle informazioni e le relative iniziative di miglioramento.
- Le responsabilità sono distribuite tra l'IT, le funzioni aziendali, le operazioni e il management in base al ruolo e alla proprietà dei processi.
- La governance viene rivista periodicamente considerando gli obiettivi aziendali, i requisiti dei clienti, gli obblighi normativi e l'evoluzione dello scenario delle minacce

2.2 Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e politiche

Prima Electro adotta un quadro documentale per il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI/ISMS). Politiche, procedure e istruzioni operative disciplinano l'uso consentito delle risorse, la classificazione delle informazioni, la gestione degli accessi, la gestione degli incidenti, il backup e la continuità operativa, la sicurezza dei fornitori e i relativi controlli.

- Le politiche e le procedure sono distribuite e rese disponibili attraverso il portale interno del SGSI.
- I requisiti di classificazione e gestione delle informazioni sono definiti per i dati e le informazioni aziendali.
- Le politiche e i controlli sono mantenuti aggiornati tramite revisioni periodiche e verifiche di conformità.

2.3 Gestione del rischio cyber e adeguamento normativo

Prima Electro è soggetta alla Direttiva NIS2 in qualità di entità importante. L'organizzazione mantiene un programma strutturato che copre la governance, la gestione del rischio cyber, la continuità operativa, la risposta agli incidenti, la sicurezza della catena di approvvigionamento, i controlli tecnici e la supervisione direzionale.

- I rischi cyber sono censiti con proprietari (*owner*) assegnati, azioni di trattamento e valutazione del rischio residuo.
- Le attività di valutazione del rischio (*risk assessment*) e di analisi dell'impatto sul business (BIA - Business Impact Analysis) supportano la definizione delle priorità per le misure di sicurezza e continuità.
- Il riesame della direzione (management review) e il monitoraggio dei controlli supportano le azioni di rimedio continue e il miglioramento costante

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

ALLINEAMENTO NIS2	Prima Electro applica un modello di governance della sicurezza basato sul rischio, allineato agli obblighi applicabili alle entità importanti, inclusi la gestione degli incidenti, la continuità operativa, la sicurezza della catena di approvvigionamento e la responsabilità della direzione

3. Sicurezza IT aziendale

3.1 Identità, controllo degli accessi e autenticazione

L'accesso ai sistemi informativi è gestito tramite account nominativi, processi di autorizzazione strutturati e la revisione periodica dei privilegi. Le richieste di accesso vengono approvate in base ai ruoli, alle esigenze aziendali e ai principi del minimo privilegio *(least privilege).*

- L'accesso remoto è limitato tramite tecnologia VPN protetta da autenticazione a più fattori (MFA).
- L'autenticazione a più fattori è applicata all'accesso remoto e ai servizi interni ed esterni in base al rischio, alla criticità e all'applicabilità tecnica.
- Le liste di controllo degli accessi (ACL) sono gestite secondo i principi del "bisogno di sapere" (*need-to-know*) e del minimo privilegio.
- L'accesso privilegiato è limitato al personale IT autorizzato e a terze parti autorizzate.
- La gestione degli accessi privilegiati (*PAM - Privileged Access Management*) è implementata per gli accessi amministrativi.
- Le operazioni amministrative sugli endpoint sono sottoposte ad audit e gestite attraverso meccanismi controllati di approvazione e di elevazione dei privilegi.

3.2 Sicurezza degli endpoint, della rete e del cloud

Prima Electro applica controlli tecnici di sicurezza multilivello su endpoint, reti, ambienti cloud e di virtualizzazione, nonché sui servizi esposti su Internet. L'architettura di sicurezza include la protezione perimetrale, reti segmentate e accessi controllati tra gli ambienti in base alla tipologia e alla criticità delle risorse.

- Gli asset endpoint e mobili sono crittografati e gestiti tramite la suite di sicurezza degli endpoint.
- Il monitoraggio e il rilascio delle patch sono supportati da strumenti automatizzati sia per gli endpoint sia per i server.
- Le attività di valutazione delle vulnerabilità (*Vulnerability Assessment*) e i test di penetrazione (*Penetration Test*) vengono eseguiti periodicamente sui sistemi informativi esposti, inclusi i livelli infrastrutturali e applicativi. Sono attive funzionalità di valutazione continua delle vulnerabilità.
- Le politiche e le procedure di sicurezza del cloud e della virtualizzazione sono documentate, approvate, comunicate, mantenute e riviste almeno su base annuale.
- I servizi esterni di MDR/XDR e la disponibilità del team IT interno supportano la risposta alle emergenze e la continuità operativa.

3.3 Gestione degli asset e protezione delle informazioni

Gli asset ICT sono tracciati tramite uno strumento di inventario dei beni (*asset inventory*), con piani di manutenzione e politiche di aggiornamento della sicurezza documentati e implementati. Le regole per il corretto utilizzo dei sistemi informativi aziendali sono definite e distribuite tramite il portale del SGSI.

- Le procedure per il ciclo di vita degli asset sono documentate per i beni ICT, e gli asset OT critici sono identificati e inventariati.
- Le politiche di classificazione delle informazioni sono definite e disponibili per l'uso da parte delle unità aziendali.
- Le informazioni e i dati digitali sono protetti in base alla loro classificazione e al livello di rischio, inclusa la crittografia ove opportuno. Le procedure di backup e ripristino vengono verificate periodicamente e includono misure quali l'immutabilità, la crittografia a riposo (*at rest*) e la replicazione off-site.

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

3.4 Monitoraggio delle vulnerabilità, delle patch e della sicurezza

Le vulnerabilità tecniche e gli aggiornamenti di sicurezza sono gestiti attraverso processi strutturati di monitoraggio, valutazione, test e implementazione. I controlli sono proporzionati all'esposizione e alla criticità del sistema.

- Strumenti automatizzati supportano il monitoraggio e il rilascio delle patch per endpoint e server.
- Valutazioni delle vulnerabilità e penetration test vengono eseguiti periodicamente sui livelli infrastrutturali e applicativi esposti.
- Gli eventi di sicurezza sono monitorati tramite funzionalità di rilevamento su endpoint, rete e servizi gestiti (*managed detection*), con escalation a specialisti interni ed esterni laddove richiesto..

3.5 Consapevolezza, formazione e sicurezza del personale

Le attività di formazione e sensibilizzazione (*awareness*) sulla cybersecurity vengono condotte in modo continuo dal 2023. Vengono eseguite periodicamente campagne simulate di phishing etico, con monitoraggio dei risultati e suggerimenti formativi specifici basati sugli esiti delle campagne e sui ruoli degli utenti.

- La formazione sulla sicurezza è continua e declinata in base al ruolo.
- Le simulazioni di phishing vengono utilizzate per identificare le esigenze formative.
- I corsi di cybersecurity specifici per ruolo sono definiti in base ai risultati dei test e alle mansioni lavorative.
- I corsi di cybersecurity sono documentati in un piano di formazione preparato e mantenuto congiuntamente da ICT e HR. Il piano viene rivisto periodicamente.

4. Resilienza operativa e gestione degli incidenti

Prima Electro mantiene un sistema di governance per gli incidenti di sicurezza delle informazioni, la gestione delle crisi, la continuità operativa (*business continuity*) e il ripristino di emergenza (*disaster recovery*). L'obiettivo è limitare l'impatto operativo, ripristinare i servizi critici e supportare una comunicazione tempestiva con le parti interessate (*stakeholder*).

- Le priorità di continuità operativa sono guidate dall'analisi dell'impatto sul business (BIA) e dalla valutazione del rischio cyber.
- Le capacità di ripristino sono supportate da procedure verificate di backup, ripristino e disaster recovery.
- Gli incidenti di sicurezza vengono segnalati, valutati, scalati e documentati secondo processi definiti.
- Ove applicabile, le notifiche sono gestite in conformità ai requisiti di NIS2, ACN (Agenzia per la Cybersicurezza Nazionale) e CSIRT, nonché agli obblighi contrattuali con gli stakeholder.
- La disponibilità dell'IT interno e il supporto di specialisti esterni contribuiscono alla risposta alle emergenze e alla continuità operativa

5. Sicurezza delle terze parti e della catena di approvvigionamento (Supply Chain)

Prima Electro riconosce la sicurezza della catena di approvvigionamento come una componente essenziale della sicurezza delle informazioni e della conformità alla Direttiva NIS2. I fornitori e i fornitori di servizi critici vengono identificati e valutati attraverso un processo basato sul rischio che considera la riservatezza, l'integrità e la disponibilità degli asset e dei servizi forniti, insieme al loro potenziale impatto sulla continuità operativa.

- I fornitori critici sono classificati in base al rischio e al potenziale impatto associati al servizio, al prodotto o all'accesso alle informazioni forniti.
- Le attività di valutazione considerano la governance, i controlli di sicurezza delle informazioni, i piani di continuità e le misure di sicurezza fisica pertinenti.
- La verifica della sicurezza dei fornitori viene mantenuta nel tempo attraverso controlli in fase di onboarding, rivalutazioni periodiche e azioni di follow-up laddove la maturità o le evidenze risultino limitate.
- I contratti includono requisiti di sicurezza delle informazioni, obblighi di riservatezza e, ove applicabile, il ribaltamento dei requisiti pertinenti lungo la catena di fornitura (flow-down).
- I fornitori di infrastrutture e servizi tecnologici, inclusi i servizi di telecomunicazione, energia e cloud, sono gestiti attraverso livelli di servizio (SLA) e aspettative di continuità definiti.

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

- Il processo di sicurezza dei fornitori viene aggiornato in caso di nuovi fornitori o di modifiche sostanziali ai servizi esistenti o all'esposizione al rischio.

6. Garanzia dei controlli, standard e miglioramento continuo

6.1 Garanzia dei controlli ed evidenze

Prima Electro riesamina periodicamente le politiche di cybersecurity, i controlli tecnici, i trattamenti del rischio e i requisiti dei fornitori. Le azioni di miglioramento vengono assegnate, monitorate e prioritizzate in base al rischio e alla rilevanza aziendale. I questionari dei clienti e le richieste di ragionevoli evidenze sono gestiti attraverso il dipartimento Digital Innovation & Security, nel rispetto dei vincoli di riservatezza e del principio del "bisogno di sapere".

- La presente relazione costituisce una sintesi della postura di sicurezza aziendale e non rappresenta un audit indipendente o un rapporto di certificazione.
- Politiche dettagliate, evidenze tecniche o impegni contrattuali possono essere forniti separatamente laddove pertinente e autorizzato.

6.2 Direttiva NIS2

Prima Electro è soggetta alla Direttiva NIS2 in qualità di entità importante. Il programma NIS2 viene utilizzato come volano per la governance, la gestione del rischio, la segnalazione degli incidenti, la continuità operativa, la sicurezza della catena di approvvigionamento e la responsabilità della direzione.

6.3 Allineamento ISO/IEC 27001

Prima Electro mantiene un quadro documentale orientato alle politiche del SGSI e implementa controlli allineati ai principi riconosciuti di gestione della sicurezza delle informazioni. La presente dichiarazione non rivendica la certificazione ISO/IEC 27001, a meno che tale certificazione non sia confermata separatamente e formalmente da Prima Electro.

Riferimento	Contesto
Direttiva (EU) 2022/2555 - NIS2	Governance, gestione del rischio, continuità, segnalazione degli incidenti e sicurezza della catena di approvvigionamento
Principi ISO/IEC 27001	Struttura del Sistema di Gestione della Sicurezza delle Informazioni e quadro dei controlli

7. Contatti e informazioni sul documento

Per richieste di informazioni sulla sicurezza, valutazioni da parte di clienti o potenziali clienti e richieste di ulteriori evidenze, si prega di contattare:

security@primaelectro.com

Questo indirizzo e-mail è stato inoltre condiviso con tutti i fornitori di Prima Electro quale punto di contatto dedicato per la segnalazione tempestiva di problematiche relative alla sicurezza delle informazioni, inclusi incidenti di sicurezza, attacchi informatici, account e-mail compromessi, violazioni di dati (*data breach*) o altri eventi che possano impattare sulle informazioni o sui sistemi di Prima Electro.

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