POLITICA PER LA SEGNALAZIONE DELLE VULNERABILITÀ E DEGLI INCIDENTI DI CYBERSECURITY

Come segnalare una sospetta vulnerabilità o un incidente di cybersecurity che interessa un prodotto Prima Electro

Informazioni	*ref.*
Versione	*1.10*
Data	*5 ottobre 2026*
Responsabile policy	*Product Security / PSIRT*
Segnalazioni	*psirt@primaelectro.com*
Destinatari	*Clienti, partner, fornitori, ricercatori di sicurezza e altri segnalanti esterni*
Classificazione	*Pubblico*

1. Finalità

Prima Electro attribuisce grande importanza alla sicurezza dei propri prodotti. La presente politica spiega come clienti, partner, fornitori, ricercatori di sicurezza e altri soggetti possano segnalare una sospetta vulnerabilità di prodotto o un incidente di cybersecurity, quali informazioni fornire e cosa aspettarsi dopo la ricezione della segnalazione.
Le segnalazioni devono essere inviate all'indirizzo psirt@primaelectro.com. Attualmente Prima Electro non utilizza un modulo web pubblico per la segnalazione di vulnerabilità o incidenti. La casella di posta elettronica è il canale ufficiale per le segnalazioni esterne disciplinate dalla presente politica.

1.1. Perimetro delle responsabilità sui prodotti

Ai fini della presente Policy, per "*Prodotti Prima Electro*" si intendono i prodotti, il software e il firmware per i quali Prima Electro opera in qualità di fabbricante oppure per i quali abbia assunto espressamente, mediante accordo scritto, obblighi di supporto in materia di cybersecurity.
La presente Politica non estende le responsabilità legali di Prima Electro oltre quanto previsto dalla normativa applicabile o dagli accordi contrattuali.

La presente Politica non estende le responsabilità legali di Prima Electro oltre quanto previsto dalla normativa applicabile o dagli accordi contrattuali.

A scanso di equivoci, **la presente Politica non si applica ai prodotti per i quali Prima Electro opera esclusivamente come fornitore di componenti, fabbricante conto terzi o fornitore di tecnologia, salvo che abbia accettato espressamente obblighi di supporto in materia di cybersecurity mediante accordo scritto**.
La ripartizione definitiva delle responsabilità per la gestione delle vulnerabilità e delle attività di conformità relative al CRA è determinata dagli accordi contrattuali applicabili e dal ruolo assunto dal pertinente operatore economico ai sensi della normativa applicabile.

2. Cosa segnalare

Contattateci se ritenete di aver individuato una vulnerabilità in un prodotto Prima Electro o se siete a conoscenza di un incidente di cybersecurity che potrebbe comprometterne la sicurezza. Se non siete certi che il problema sia pertinente, segnalatelo e spiegate perché ritenete che possa avere un impatto sulla sicurezza.

Tipo di segnalazione	Esempi
Vulnerabilità del prodotto	Debolezze nei meccanismi di autenticazione o autorizzazione, comunicazioni non sicure, servizi esposti, vulnerabilità di tipo injection, problemi di sicurezza della memoria, escalation dei privilegi, modalità di aggiornamento non sicure, debolezze crittografiche o componenti di terze parti vulnerabili.
Incidente di cybersecurity	Sospetta compromissione, accesso non autorizzato, manipolazione dolosa, perdita di disponibilità, integrità o riservatezza, indicatori di sfruttamento o comportamenti anomali plausibilmente riconducibili a un evento di sicurezza.
Informazioni sulla catena di fornitura	Vulnerabilità o incidenti che interessano software, firmware, librerie, sistemi operativi, servizi o componenti integrati in un prodotto Prima Electro o utilizzati con esso.

2.1. Modifiche apportate dai clienti o da terzi

Prima Electro valuta le vulnerabilità che interessano la configurazione standard dei propri prodotti.

Quando le vulnerabilità derivano esclusivamente da software, firmware, hardware o configurazioni introdotti dai clienti o da terzi senza l'autorizzazione di Prima Electro, la responsabilità di tali modifiche resta in capo al soggetto che le ha implementate.
Ove ragionevolmente necessario, Prima Electro può comunque collaborare alla valutazione di tali vulnerabilità e al coordinamento della loro gestione.

3. Segnalazione di un incidente di cybersecurity

In caso di incidente in corso o sospetto, indicatelo chiaramente nell'oggetto dell'e-mail.
La segnalazione al PSIRT non sostituisce gli eventuali canali di notifica previsti per le emergenze, la sicurezza, gli obblighi contrattuali o gli obblighi di legge applicabili al segnalante. In presenza di un rischio immediato per le persone, i beni o le operazioni essenziali, seguite innanzitutto le procedure applicabili per le emergenze e la sicurezza del sito; successivamente, trasmettete al PSIRT le informazioni di cybersecurity disponibili.

4. Come effettuare una segnalazione

Per segnalare una sospetta vulnerabilità o un incidente di cybersecurity che interessa un prodotto Prima Electro, compilate l'apposito modulo direttamente sul nostro sito web.

Non inserite nel modulo o nell'e-mail iniziale password, chiavi private, dati personali non necessari, dati di produzione dei clienti o altre informazioni segrete. Se il materiale di supporto è sensibile o troppo voluminoso per l'invio via e-mail, indicatelo nel modulo e chiedete al PSIRT di Prima Electro istruzioni per il trasferimento sicuro.

Per aggiornare una segnalazione già inviata, rispondete alla conversazione e-mail originale.

5. Linee guida per la divulgazione responsabile

Chiediamo a chi effettua segnalazioni e ai ricercatori di agire in buona fede e di evitare di causare danni. Durante l'analisi o la verifica di una sospetta vulnerabilità:

- testate esclusivamente sistemi e prodotti di vostra proprietà o per i quali disponete di un'autorizzazione esplicita;
- utilizzate il livello minimo di accesso e i dati strettamente necessari per dimostrare il problema;
- interrompete i test e segnalate immediatamente il caso se vi imbattete in dati personali, informazioni riservate, dati di produzione o prove di una compromissione in corso;
- non modificate, cancellate, conservate né divulgate dati che non vi appartengono;
- non compromettete la disponibilità, non interrompete le operazioni, non interferite con le funzioni di sicurezza e non eseguite test di tipo denial of service;
- non ricorrete a tecniche di ingegneria sociale, phishing, intrusione fisica o attacchi contro dipendenti, clienti, fornitori o altri soggetti terzi;
- non installate strumenti, non eseguite movimenti laterali, non esfiltrate informazioni e non utilizzate quanto rilevato per ottenere vantaggi commerciali o personali;
- concedete a Prima Electro un tempo ragionevole per analizzare e risolvere il problema prima di divulgarlo pubblicamente;
- coordinate con il PSIRT di Prima Electro i tempi e i contenuti di qualsiasi divulgazione.

6. Gestione delle segnalazioni

Dopo aver ricevuto una segnalazione, Prima Electro valuta se il problema riguarda un proprio prodotto, la assegna per l'analisi e contatta il segnalante qualora siano necessari chiarimenti o ulteriori elementi. A seconda del caso, l'analisi può coinvolgere le funzioni Sicurezza dei prodotti, Ingegneria, Qualità, Assistenza clienti, Legale o altre funzioni pertinenti.

1. **Ricezione e conferma.** Il PSIRT registra la segnalazione e, quando sono disponibili i recapiti, si impegna a confermarne la ricezione. La conferma attesta esclusivamente l'avvenuta ricezione e non convalida la segnalazione né ne conferma la gravità o la rilevanza ai fini normativi.
2. **Triage e convalida.** I team competenti valutano il prodotto e le versioni interessate, la riproducibilità, le evidenze di sfruttamento della vulnerabilità, la gravità, l'impatto e le misure di mitigazione disponibili.
3. **Coordinamento.** Prima Electro può richiedere ulteriori informazioni, fornire indicazioni provvisorie o coordinare con il segnalante e le parti interessate le attività di test e divulgazione.
4. **Risoluzione e comunicazione.** Ove opportuno, Prima Electro sviluppa misure correttive o di mitigazione e definisce le comunicazioni necessarie a clienti, partner o pubblico.
5. **Chiusura**. Prima Electro registra l'esito e può informare il segnalante al termine dell'indagine o quando è possibile condividere informazioni.

I tempi di risposta e di risoluzione dipendono dalla complessità e dalla gravità del caso, dai prodotti interessati, dalla disponibilità di evidenze e dal coordinamento necessario. La presente Politica non garantisce tempi specifici di risposta o risoluzione.
Le attività di conferma della ricezione, indagine, valutazione e risoluzione descritte nella presente Politica non costituiscono livelli di servizio contrattuali e non devono essere interpretate come un impegno relativo ai livelli di servizio, salvo espresso accordo scritto.

6.1. Coordinamento con fornitori e provider tecnologici

Qualora una vulnerabilità segnalata interessi componenti, sistemi operativi, librerie o servizi forniti da terzi, Prima Electro può coordinare le attività di indagine e risoluzione con i fornitori, i fabbricanti o i provider tecnologici interessati.
Nel valutare l'impatto della vulnerabilità, la disponibilità di misure di mitigazione e i tempi di risoluzione, Prima Electro può fare affidamento sulle informazioni fornite da tali soggetti.

7. Riservatezza e divulgazione coordinata

Prima Electro gestisce le informazioni ricevute in funzione delle esigenze di indagine, mitigazione e adempimento degli obblighi applicabili. Tali informazioni possono essere condivise all'interno di Prima Electro e con società affiliate, fornitori, clienti, prestatori di servizi, autorità competenti o altri soggetti, quando necessario per tali finalità e nel rispetto di misure di controllo adeguate.
I segnalanti sono tenuti a mantenere riservate le informazioni non pubbliche relative a vulnerabilità e incidenti finché non sia stato concordato un piano di divulgazione o il problema non sia stato altrimenti affrontato. Una richiesta di riservatezza non può impedire divulgazioni imposte dalla legge o necessarie a proteggere gli utenti e i sistemi interessati.

8. Ricerca in buona fede e considerazioni legali

Prima Electro riconosce il valore della ricerca di sicurezza svolta in buona fede e nel rispetto della presente Politica. Nel valutare l'attività, Prima Electro terrà conto del rispetto della Politica da parte del segnalante e intende non promuovere azioni esclusivamente per attività di ricerca accidentali e svolte in buona fede, segnalate tempestivamente e che non abbiano causato danni evitabili.
La presente Politica non autorizza l'accesso a sistemi o dati di terzi, non deroga alle restrizioni contrattuali o legali applicabili e non vincola i soggetti terzi. I segnalanti restano responsabili del rispetto della normativa applicabile e dell'ottenimento di ogni autorizzazione necessaria. La presente Politica non costituisce un programma bug bounty e non attribuisce alcun diritto a compensi, premi, riconoscimenti pubblici o rapporti di lavoro.

9. Privacy

Prima Electro utilizza i dati personali forniti con una segnalazione per comunicare con il segnalante, indagare sul problema, proteggere i prodotti e gli utenti, adempiere agli obblighi di legge e conservare la relativa documentazione di sicurezza. Fornite esclusivamente informazioni pertinenti alla segnalazione e che siete autorizzati a condividere.
I dati personali trasmessi ai sensi della presente Politica saranno trattati in conformità all'Informativa Privacy applicabile di Prima Electro, come periodicamente aggiornata.
Ulteriori informazioni sul trattamento dei dati personali, inclusi l'identità del titolare del trattamento e i diritti riconosciuti agli interessati dalla normativa applicabile in materia di protezione dei dati, sono disponibili nell'Informativa Privacy applicabile.

10. Esclusioni dal perimetro

La presente Politica riguarda le sospette vulnerabilità e gli incidenti di cybersecurity che interessano i prodotti Prima Electro. Le richieste generali di supporto tecnico, i difetti funzionali privi di un plausibile impatto sulla sicurezza, le richieste commerciali e i reclami non connessi alla cybersecurity devono essere indirizzati ai canali di assistenza o ai contatti aziendali appropriati di Prima Electro.

10.1. Prodotti fuori commercio e fine vita

Prima Electro può classificare i prodotti come End of Sale (EOS, fine commercializzazione) o End of Life (EOL, fine vita) mediante comunicazioni specifiche ai clienti o avvisi pubblicati.
Il supporto del prodotto, il monitoraggio delle vulnerabilità e gli obblighi relativi agli aggiornamenti di sicurezza sono disciplinati dal periodo di supporto dichiarato da Prima Electro o altrimenti concordato per iscritto.
Dopo la scadenza del periodo di supporto applicabile, Prima Electro può limitare le attività di gestione delle vulnerabilità nei limiti consentiti dalla normativa applicabile.

11. Contatti

Finalità	*Contatto*
Segnalare una sospetta vulnerabilità del prodotto o un incidente di cybersecurity relativo a un prodotto	*psirt@primaelectro.com*
Aggiornare una segnalazione esistente	*Rispondere alla conversazione e-mail esistente, mantenendo l'oggetto originale e il riferimento, se fornito.*

12. Aggiornamento della Policy

Prima Electro può aggiornare la presente Politica per riflettere modifiche ai prodotti, ai canali di segnalazione, ai requisiti di legge e alle pratiche di sicurezza.
La versione pubblicata più recente sostituisce le versioni precedenti.