Coordinated Vulnerability Disclosure Policy (CVD Policy)

Field	Details
Document Owner	**PSIRT**
Version	**1.0**
Effective Date	**September 3, 2026**
Last Review Date	**September 2, 2026**
Next Review Date	**August 21, 2027**
Review Cycle	Annually, or after major changes
Classification	Public

1. Purpose

Kinco Electric (Shenzhen)Ltd. (hereinafter referred to as "the Organization") is committed to ensuring the security of its products containing digital elements, in compliance with the requirements of the EU Cyber Resilience Act (Regulation (EU) 2024/2847).

This Coordinated Vulnerability Disclosure (CVD) Policy sets forth the process by which external security researchers, customers, suppliers, coordinators, and the public may report potential security vulnerabilities in the Organization's products, and defines the Organization's commitments in handling and disclosing such vulnerabilities.

This Policy is developed in accordance with **EN 40000-1-3:2025** (Cybersecurity Requirements — Vulnerability Handling), which establishes requirements and recommendations for manufacturers of products containing digital elements in vulnerability handling and disclosure.

This CVD Policy is publicly available on the Organization's official website: https://automation.kinco.cn/security/CVD_Policy.pdf

The policy is provided in an accessible digital format. The Organization ensures that the published policy can be accessed without authentication and can be reasonably understood by security researchers and stakeholders.

2. Definition of Terms

Term	Definition
Vulnerability	A weakness in a product containing digital elements that can be exploited by a threat actor

Term	Definition
Security Update	A patch, fix, upgrade, or mitigation measure used to remediate a confirmed vulnerability
SBOM (Software Bill of Materials)	A machine-readable inventory of software components contained in a product, documenting at least top-level dependencies
Coordinator	An independent entity that facilitates communication between the reporter and the manufacturer in multi-party vulnerability disclosure
Embargo Period	An agreed timeframe during which vulnerability information remains confidential prior to public disclosure
Traffic Light Protocol (TLP)	A set of designations used to ensure that sensitive information is shared only with the appropriate audience
Reporter	Any individual or organization that identifies and submits a potential vulnerability

3. Scope

3.1 Applicable Products and Services

This Policy applies to all **industrial automation control products and supporting software** independently developed, manufactured, and sold by the Organization, including but not limited to the following product lines:

- **Human-Machine Interface (HMI) Series**: including touch panels and related configuration software;
- **Programmable Logic Controller (PLC) Series**: including various models of logic control modules and programming environments;
- **Servo Drive and Motion Control Series**: including servo drives, servo motors, and debugging software;
- **Supporting Industrial Software and Cloud Platforms**: including client/server software, Apps, and cloud service platforms used for device management and data monitoring.

3.2 Out of Scope

The following are explicitly excluded from this Policy:

- Third-party products, services, or infrastructure not owned or operated by the Organization
- Social engineering, phishing, or physical security attacks
- Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks
    - Denial-of-Service vulnerabilities are considered within scope when they affect the security or availability of supported products. Purely theoretical availability concerns without practical impact may be excluded.
- Vulnerabilities in products that have reached end-of-life and are no longer supported by the Organization
- Issues previously reported to the Organization that are already known or under active remediation

3.3 Software Bill of Materials (SBOM)

The Organization maintains a Software Bill of Materials (SBOM) for its products containing digital elements, in a machine-readable format documenting at least top-level dependencies, in accordance with Regulation (EU) 2024/2847 Annex I Part II (b). The SBOM is used internally to support vulnerability identification and impact assessment.

3.4 Handling Vulnerabilities in Third-Party and Upstream Components

Where a reported vulnerability affects a third-party or open-source component embedded in the Organization's products, the Organization shall:

- Identify the affected component and assess its impact on the product;
- Coordinate remediation with the component vendor or upstream provider; and
- Notify relevant upstream product providers of the vulnerability in accordance with applicable laws and regulations.

The Organization maintains internal records of the software components used in its products to support these activities; detailed software component and SBOM management is governed by the Organization's internal **Vulnerability Handling Policy** and related supply-chain procedures.

---

4. Roles and Responsibilities

4.1 Product Security Incident Response Team (PSIRT)

The designated external interface team responsible for managing vulnerability disclosure is the **Product Security Incident Response Team (PSIRT)**. Toward reporters, this team is responsible for:

- Receiving and acknowledging vulnerability reports
- Classifying, investigating, and prioritizing reported vulnerabilities
- Coordinating remediation efforts with relevant internal teams and upstream stakeholders (where applicable)
- Identifying affected software components to support impact assessment and remediation
- Maintaining communication with the reporter throughout the process
- Publishing security advisories or notifications as appropriate
- Maintaining records of all vulnerabilities handled

> **Note:** The internal organizational framework and detailed role responsibilities involved in vulnerability handling (including product R&D, testing teams, product owners, quality departments, legal/compliance, supply chain management, security update release approvers, and escalation leads for critical vulnerabilities) are defined in the Organization's internal **Vulnerability Handling Policy**. In this Policy, PSIRT serves as the external single point of contact and coordination interface.
>
> The **CVD Policy** shall be implemented together with the internal **Vulnerability Handling Policy**.

4.2 Reporter

Any individual or organization that identifies and submits a potential vulnerability. Reporters shall:

- Act in good faith and comply with the terms of this Policy
- Avoid unauthorized access to or modification of data or systems
- Refrain from publicly disclosing the vulnerability before the Organization has had a reasonable opportunity to remediate it
- Provide sufficient detail to enable the Organization to reproduce and verify the issue

4.3 Safe Harbor

The Organization will not initiate legal action against reporters who act in good faith and in compliance with this Policy, including for activities such as accessing the Organization's publicly available products for the sole purpose of identifying and reporting vulnerabilities. Good-faith security research and responsible disclosure conducted in accordance with this Policy shall not give rise to legal liability.

This Safe Harbor does not apply to activities that:

- involve unauthorized access to data or systems beyond what is necessary to verify a reported vulnerability;
- cause damage or disruption to the Organization's products or services;
- are conducted for malicious purposes or personal gain; or
- violate applicable law.

---

5. How to Report a Vulnerability

5.1 Submission Channels

Vulnerability reports shall be submitted through the following channels:

Channel	Details
Email	security@kinco.cn
Customer Service	400 700 5281

security.txt (Machine-Readable Contact Entry): The security.txt file is a machine-readable security contact file published in accordance with RFC 9116, enabling security researchers and automated tools to quickly locate the Organization's vulnerability reporting channels, encryption public key, and security policy. File location: **https://www.kincoautomation.com/.well-known/security.txt**.

5.2 Report Content

To facilitate efficient triage, reporters should provide the following information to the best of their ability:

1. **Affected Product**: Product name, version, platform, and/or URL
2. **Vulnerability Description**: Detailed description of the vulnerability and its potential impact

3. **Reproduction Steps**: Step-by-step instructions, including tools and environment details
4. **Supporting Evidence**: Screenshots, network packet captures, logs, or Proof-of-Concept (PoC) code
5. **Severity Assessment**: Suggested CVSS v3.1 or v4.0 score (optional)
6. **Contact Information**: Email or other contact information for follow-up communication

---

6. Secure Communication

6.1 Supported Secure Communication Methods

Method	Purpose
S/MIME or OpenPGP-encrypted email	For exchanging sensitive vulnerability details

Reporters may initially submit vulnerability information through available channels.When sensitive information is required, communication should be transferred to a secure communication channel.

Security researchers may encrypt sensitive vulnerability information using the Organization's OpenPGP public key:
Public Key: https://www.kincoautomation.com/.well-known/pgp-key.asc
PGP Key Fingerprint: B068EFB9661FF1994A1C7B064AF830B11D0F55F1

6.2 Operational Security

All non-public vulnerability information is treated as confidential. Access is limited to authorized PSIRT members and relevant stakeholders on a need-to-know basis. Information may be classified using the Traffic Light Protocol (TLP):

TLP Level	Meaning
TLP:RED	For designated recipients only — not to be shared beyond designated recipients
TLP:AMBER	Limited disclosure — Organization and its stakeholders only
TLP:GREEN	Community-wide disclosure — shared within the community
TLP:CLEAR	Unlimited disclosure — may be shared without restriction

---

7. Ongoing Communication

7.1 Communication Commitments

The Organization follows its internal **Vulnerability Handling Policy** to validate, risk-assess, remediate, and release fixes for reported vulnerabilities, and commits to maintaining regular communication with reporters and stakeholders throughout the handling process:

- **Acknowledgement**: Within **5** business days of receipt, with assignment of a unique tracking number (e.g., **KINCO-YYYY-NNNN**)
- **Status Updates**: At least once every **30** calendar days during active handling

- **Validation Results**: Provided upon completion of initial assessment
- **Remediation Timeline**: Communicated upon completion of risk assessment
- **Resolution Notification**: Provided when the fix is released
- **Public Announcements**: Published through the Organization's security channels

Communication channels include email, customer service phone, and other appropriate accessible modes.

The communication frequency and content may be adjusted based on:

- vulnerability severity
- affected products
- disclosure agreements
- involvement of third parties

7.2 Coordinated Disclosure and Embargo Period

The Organization supports coordinated public disclosure. Prior to any public disclosure, both parties shall agree on:

- The disclosure date
- The content of any public announcement or statement
- The embargo period required to protect users

During the agreed embargo period, vulnerability information shall be kept confidential by both parties and shall not be disclosed to third parties not involved in the coordination.

> **Note:** Different embargo periods may be negotiated on a case-by-case basis between the Organization and the reporter (or involving a coordinator, where applicable).

The Organization aims to complete coordinated disclosure within a coordinated disclosure window not exceeding **90** calendar days from the date of acknowledgement. If completion within this window is not possible, the reporter will be notified and a revised date will be mutually agreed.

7.3 Coordinated Disclosure Process

The coordinated disclosure process generally follows:

- Report submission
- Initial acknowledgement
- Vulnerability validation
- Risk assessment
- Remediation development
- Security update release
- Public disclosure

The Organization coordinates disclosure timing with reporters and affected stakeholders when appropriate.

7.4 Security Update Provision

Security updates — meaning software or firmware updates (e.g., patches, fixes, or mitigation measures) issued to remediate vulnerabilities covered by this Policy — are provided **free of charge** to users of supported products, together with an accompanying security advisory.

---

8. Confidentiality

8.1 Confidentiality Commitments

The Organization will keep vulnerability reports confidential and will not share reporters' personal information with third parties without explicit consent, except as required by applicable law.

Non-public vulnerability information will be handled in accordance with the operational security measures defined in Section 6.2.

Reporters who wish to remain anonymous may do so; however, anonymity may limit the Organization's ability to provide follow-up communication or recognition.

8.2 Data Protection

The Organization processes reporters' personal data in accordance with the **General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR")** for reporters located in the European Economic Area and the **Personal Information Protection Law of the People's Republic of China ("PIPL")** for reporters located in China, as applicable.

- **Data Controller**: The Organization, as defined in Section 1, is the data controller for personal data submitted through the vulnerability reporting channels.
- **Legal Basis**: Personal data is processed on the basis of the Organization's legitimate interest in receiving, evaluating, and remediating reported security vulnerabilities, and/or to take steps prior to entering into a contract with the reporter where applicable.
- **Data Categories**: Contact information (e.g., name or alias, email address) and any other personal data voluntarily provided in the report.
- **Retention Period**: Personal data is retained for the duration of the vulnerability handling process and, where a security advisory is published, for as long as needed to maintain public security records in accordance with applicable law.
- **Data Subject Rights**: Reporters may exercise their rights of access, rectification, erasure, restriction of processing, data portability, and objection by contacting **security@kinco.cn**. The Organization will respond within the timeframe required by applicable law.
- **Legal Exception Disclosure**: Where the Organization is required by applicable law to disclose reporter personal information (e.g., pursuant to a court order or statutory obligation), disclosure will be limited to the minimum information required and the reporter will be notified to the extent permitted by law.

---

9. Acknowledgment and Rewards

The Organization **does not operate** a bug bounty program. However, the Organization highly values the contributions of security researchers who responsibly disclose valid vulnerabilities.

Researchers who comply with this Policy may be eligible for:

- **Public acknowledgment** in the corresponding security advisory or fix announcement, unless the researcher requests to remain anonymous. The acknowledgment may include the researcher's name or alias, as preferred.
- Commemorative gifts or other non-monetary recognition, at the Organization's sole discretion.

Any rewards or acknowledgments offered are at the Organization's sole discretion and are contingent upon the reporter's full compliance with the terms of this Policy. Reports that violate any provision of this Policy shall not be eligible for acknowledgment or rewards.

---

10. Contact Information

Field	Details
Security Contact	**security@kinco.cn**
PGP Public Key	**https://www.kincoautomation.com/.well-known/pgp-key.asc**
Response Hours	**Monday to Friday, 09:00 – 18:00 Beijing Time (UTC+8), excluding public holidays**
security.txt	**https://www.kincoautomation.com/.well-known/security.txt**
Customer Service	400 700 5281

---

11. Policy Management

11.1 Review and Updates

This Policy will be reviewed at least annually, or following significant changes to the Organization's products, regulatory environment, or threat landscape. Updates will be published on the Organization's website and communicated internally.

11.2 Exceptions

Any exceptions to this Policy must be formally approved by the document owner and recorded in an exception register. Exceptions are time-limited and subject to annual review.

11.3 Compliance Evidence

The Organization maintains the following evidence to demonstrate compliance with this Policy and EN 40000-1-3:

- Published CVD Policy (this document)
- Publicly accessible evidence of contact mechanisms
- Records of acknowledged reports with tracking numbers
- Documentation of validation and risk assessments

- Remediation plans and timelines
- Remediation test reports
- Published security advisories
- Communication records with reporters and stakeholders

---

12. Governing Law and Jurisdiction

This Policy shall be governed by and construed in accordance with the laws of the **People's Republic of China**, without regard to its conflict of law rules.

Any dispute arising out of or in connection with this Policy shall first be resolved through friendly negotiation. If no resolution can be reached within thirty (30) days, the dispute shall be submitted to the competent court at the location where the Organization is domiciled for adjudication.

Nothing in this Policy shall be construed as a waiver of, or limitation on, the Organization's obligations under the EU Cyber Resilience Act (Regulation (EU) 2024/2847), EN 40000-1-3, or any other applicable mandatory laws and regulations.

Appendix A: Vulnerability Report Template

Reporters may use the following template when submitting a vulnerability:

Field	Description
Reporter Name/Alias	{Name or alias}
Contact Email	{Email for follow-up communication}
Affected Product	{Product name and version}
Vulnerability Type	{e.g., SQL injection, buffer overflow, XSS}
CVSS Score (if known)	{e.g., CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H}
Description	{Detailed description of the vulnerability}
Reproduction Steps	{Step-by-step instructions}
Environment Information	{OS, browser, configuration details}
Supporting Evidence	{Screenshots, PoC code, logs}
Suggested Mitigations	{Optional: suggested remediation approach}
Disclosure Preferences	{e.g., credited in announcement, anonymous}

Appendix B: Document Revision History

Version	Date	Author	Change Description
1.0	**September 2, 2026**	**PSIRT**	Initial release