Docusign Envelope ID: DF2DE2FF-2791-4B15-81DB-F10A31C953E2

SUBNET Solutions Inc.
Vulnerability Disclosure Policy

DVPO-004
Rev. 0

DOCUMENT SIGNOFF

Approver	Name	Signature	Date (MMM.DD.YYYY)
Chief Technical Officer	Anthony Eshpeter	Signed by: Anthony Eshpeter 03D39BCA6BCC4B7...	1/6/2026
Chief Cyber Security Architect	Kelly Stich	Signed by: Kelly Stich 602AED688BFE4FB...	1/5/2026

MODIFICATION RECORD

Rev.	Change Description	Author	Date
0	Initial release	Kelly Stich	2025-12-17

INFORMATION PROTECTION POLICY

This document is classified according to SUBNET's Information Protection Policy as TLP:CLEAR, defined by FIRST as:

> Recipients can spread this to the *world*, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

As such, this document is able to be shared with our clients publicly. This document is protected by copyright, and is the exclusive property of SUBNET Solutions Inc. You may not reproduce, copy, modify, or publish the material contained herein without prior written authorization from SUBNET Solutions Inc.

Docusign Envelope ID: DF2DE2FF-2791-4B15-81DB-F10A31C953E2

SUBNET Solutions Inc.
Vulnerability Disclosure Policy

DVPO-004
Rev. 0

1.0 Purpose of Policy

SUBNET Solutions Inc., hereafter referred to as SUBNET, has established and implemented processes to receive, analyze and respond to, and disclose vulnerabilities reported to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

2.0 Scope

This policy is effective for all software products created by SUBNET. SUBNET's vulnerability disclosure policy is designed to be consistent with the CISA coordinated vulnerability disclosure process (formerly ICS-CERT).

3.0 Vulnerability Detection

3.1 By SUBNET

3.1.1 SUBNET has a Vulnerability Detection and Remediation Policy that outlines our internal requirements. Contact cybersecurity@subnet.com to request access to this policy.

3.2 By Third-Parties

3.2.1 Anyone can report a potential vulnerability to SUBNET at cybersecurity@SUBNET.com. Alternatively, anyone can report a potential vulnerability to the Vulnerability Information and Coordination Environment (VINCE) operated by the Software Engineering Institute at Carnegie Mellon University, accessible at https://kb.cert.org/vince/, including anonymous submissions.

3.2.2 SUBNET recommends penetration testing of all client deployments. Any vulnerabilities discovered within this process will be assessed and verified based on our Vulnerability Detection and Remediation Policy. If verified, SUBNET will follow the process identified herein for disclosure.

3.2.2.1 Clients should test the system as configured in the production environment prior to go-live. Testing of an active production system or operational assets should not be performed.

3.2.3 SUBNET will assess vulnerabilities that impact our software products.[1]

[1] Vulnerabilities related to the operating system, identity management platform, other third-party components of the system, or configuration issues will not be addressed, nor will vulnerabilities that require social engineering, administrator access to the operating system, or physical access to the system, unless they uncover flaws in our products requiring remediation.

Docusign Envelope ID: DF2DE2FF-2791-4B15-81DB-F10A31C953E2

SUBNET Solutions Inc.
Vulnerability Disclosure Policy

DVPO-004
Rev. 0

4.0 Vulnerability Disclosure Policy

4.1.1 SUBNET follows the CISA coordinated vulnerability disclosure process. This process follows five basic steps: 1) Collection of Information; 2) Analysis of Vulnerability Report; 3) Mitigation/Update Coordination; 4) Application of Mitigation/Update, and 5) Public Disclosure. A reasonable timeframe for the disclosure will be reached depending on factors listed by CISA, with a minimum of 45 days from initial report to public disclosure to allow time to investigate and resolve any vulnerabilities that are discovered.

4.1.2 SUBNET will disclose vulnerabilities publicly via CISA CVE Numbering Authority (CNA).

4.1.3 SUBNET will disclose to Clients all confirmed vulnerabilities related to the products or services within two days of public disclosure.

4.1.4 SUBNET's vulnerability disclosure notifications to Clients will include:

4.1.4.1 A description of each vulnerability and material defect;

4.1.4.2 its potential impact;

4.1.4.3 the root cause;

4.1.4.4 status of SUBNET's efforts to mitigate;

4.1.4.5 recommended corrective actions;

4.1.4.6 compensating security controls;

4.1.4.7 mitigations, and

4.1.4.8 procedural workarounds.

4.1.5 Client notifications will be sent from securitynotifications@subnet.com

4.1.6 When publicly released, SUBNET vulnerability disclosures will be posted to the CISA ICS Advisories, https://www.cisa.gov/news-events/ics-advisories, and SUBNET's trust center, https://trust.subnet.com.

4.1.7 CISA makes available machine-readable Common Security Advisory Framework (CSAF) records at https://github.com/cisagov/CSAF.

Docusign Envelope ID: DF2DE2FF-2791-4B15-81DB-F10A31C953E2

4.2 Vulnerability Disclosure Classifications

4.2.1 SUBNET employs the following classifications within our disclosures:

Traffic Light Protocol Label for Notification	Description of Vulnerability Notification	Disclosure Process
TLP:RED	• Vulnerability exploitation detected • Intended for CIP-013 R1.2.2 Coordination of responses for product-related security	• Advanced email notification, sent within four hours of confirmation • Sent to all subscribed clients and Incident Response Contacts • Triggers CVE assignment
TLP:AMBER	• Vulnerability has been identified, and an update is being developed • Intended for CIP-013 R1.2.2 Coordination of responses for product-related security • Should not be used for CIP-007 R2.1 patch source	• Advanced email notification, sent within two days of CVE assignment • Sent to clients that have requested advance notification • Triggers CVE assignment
TLP:GREEN	• Vulnerability notification upon software update release • Intended for CIP-013 R1.2.4. Disclosure by vendors of known vulnerabilities related to the products • May be used for CIP-007 R2.1 patch source, as per entity process NOTE: please use the *Public disclosure date* under section *Vulnerability Disclosure Policy* as the software release date	• Email notification on release • Sent to all subscribed clients • CVE will not be assigned if only third-party libraries are updated
TLP:CLEAR	• Monthly Security Bulletins • May be used for CIP-007 R2.1 patch source, as per entity process	• Email at month end • Posted to our trust center

Table 1 Vulnerability Disclosure Classifications

Docusign Envelope ID: DF2DE2FF-2791-4B15-81DB-F10A31C953E2

4.2.2 SUBNET uses the following update codes in software release notes and vulnerability disclosures for Minor Releases:

Update Code	Description
[Security: Optional Update]	This category indicates an update to address vulnerabilities that have minimal to no impact on a properly configured system. Third-party components with vulnerabilities, that do not impact our software, have been updated as best practice.
[Security: Recommended Update]	This category indicates an update considered important for continued secure use of the system. This indicates that a software vulnerability was discovered and remediated or security enhancement was made to the software. There is High or Medium severity CVE either assigned to the software, or assigned to a third-party component affecting product security.
[Security: Critical Update]	Updates in this category are considered necessary for secure use of the system. This usually indicates that a problem was fixed that may jeopardize the security, safety, performance, or stability of the application. There is a Critical severity CVE assigned to the software, or assigned to a third-party component affecting product security.

Table 2 Update Code Classifications

4.3 Vulnerability Disclosure to Authorities

4.3.1 SUBNET reports vulnerabilities to CISA via VINCE as specified in 3.2.1 .

4.3.2 Clients may disclose, without negative action or consequence from SUBNET, any TLP:RED vulnerabilities or material defects in the products and services provided by SUBNET to any of the following:

4.3.2.1 The Electricity Information Sharing and Analysis Center (E-ISAC), the European Electricity Information Sharing and Analysis Center (EE-ISAC), the Cybersecurity and Infrastructure Security Agency (CISA, formerly Industrial Control Systems Cyber Emergency Response Team, ISC-CERT), European Union Agency for Cybersecurity (ENISA), or any equivalent entity;

Docusign Envelope ID: DF2DE2FF-2791-4B15-81DB-F10A31C953E2

4.3.2.2 Any entity when necessary to preserve the reliability of the Bulk Electric System; and

4.3.2.3 Any entity required by applicable law.

4.3.3 Clients must not disclose TLP:AMBER advanced notice vulnerability disclosures while under embargo, until such time as SUBNET's stated *Public disclosure date* in the notification under section *Vulnerability Disclosure Policy* has elapsed. These are confidential while SUBNET is working towards a solution, to limit public awareness of the vulnerability before remediation can be completed.

4.3.4 SUBNET requests that clients attempt to contact us prior to any disclosures under 4.3.2