SUBEX

Vulnerability Disclosure Policy.

1.0 | Wednesday, July 23, 2025

Revision History

Sl. No.	Revision Date	New Version Number	Change Description	Page Numbers Affected	Reference – Change Request Form	Prepared By	Approved By
01	07-Jul-2025	1.0	Baseline	ALL	-	Rahul J Alexander	Kamesh Babu
02	9-Jul-2025	1.1	Indexing	All	-	Manohar	Kamesh Babu

Table of Contents

1 Purpose of Policy

Subex Limited ("the Company") is committed to maintaining the security and integrity of our public-facing applications and infrastructure. This policy provides a comprehensive framework for security researchers and the public to responsibly discover and report vulnerabilities in our systems. The aim is to protect the confidentiality, integrity, and availability of Company assets and ensure compliance with relevant laws, regulations, and industry standards.

2 Scope of Policy

This policy applies to all public-facing applications and internet accessible systems owned or operated by Subex Limited. This explicitly includes, but is not limited to, web applications, APIs, online services, and related infrastructure.

Particular attention is given to systems that:

- Handle, store, or transmit Company confidential or sensitive data (e.g., customer data, intellectual property, financial data, employee PII).
- Provide critical services or infrastructure essential to the Company's operations.
- Have access to Company systems, networks, or physical facilities.
- Internal systems, non-public environments, and physical security vulnerabilities are generally out of scope for direct testing under this policy, except where specifically authorized.

3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply:

Term	Definition
Company	Referring to Subex Ltd. and all its subsidiaries.
Third Party	Any external entity (individual or organization) that provides services, software, hardware, or data processing capabilities to the Company, including vendors, suppliers, consultants, cloud service providers, contractors, and partners.
Sensitive Data	Any information that, if compromised, could lead to significant harm to the Company, its customers, or employees. This includes, but is not limited to, Personally Identifiable Information (PII), Protected Health Information (PHI), financial data, intellectual property, trade secrets, and confidential business strategies.
Critical Service/System	A service or system whose disruption or compromise would have a severe impact on the Company's ability to operate, meet its legal or contractual obligations, or maintain its reputation.
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
Researcher	An individual or group that discovers and reports a potential security vulnerability.
In-Scope Systems	Public-facing applications and internet accessible systems owned or operated by Subex Limited.

4 Reporting Vulnerabilities

If you discover a security vulnerability within the defined scope, please report it by emailing us at cyber.security@subex.com.

Please include the following information in your report:

- A clear and concise description of the vulnerability
- Detailed steps to reproduce the issue, including URLs, parameters, and payloads.
- The potential impact of such vulnerability.
- Any supporting evidence (e.g., screenshots, logs, code samples, proof-of-concept exploits etc.)
- Your contact information for follow-up communication.

5 Response Process

We pledge to:

- Acknowledge receipt of your report within the timeframe specified in the Vulnerability Response Matrix.
- Evaluate and verify the issue promptly
- Provide updates as necessary during the remediation process, as per the frequency defined in the Vulnerability Response Matrix.
- Work to resolve verified vulnerabilities in a timely manner, adhering to the service level agreements outlined in the Vulnerability Response Matrix.
- Communicate the resolution and closure of the issue to the reporter (if known and permitted).

6 Safe Harbor

If you adhere to this policy in good faith and conduct your activities in a lawful and ethical manner, Subex Limited will not initiate legal action against you. This includes good-faith, accidental violations of the policy that are immediately reported to Subex.

To qualify for safe harbor, researchers must:

- Adhere to all applicable laws and regulations during their vulnerability research activities.
- Avoid accessing or modifying data beyond what is necessary to demonstrate vulnerability.
- Not cause significant harm to the Company, its customers, or employees, or a severe impact on the Company's ability to operate, meet its legal or contractual obligations, or maintain its reputation.
- Avoid actions that could compromise the privacy or security of Subex customers or data.
- Not engage in physical security testing, social engineering, or Denial of Service (DoS) attacks.
- Not disclosing vulnerability details publicly until Subex has had a reasonable opportunity to address the issue, as outlined in the Coordinated Disclosure section. Any activities not in line with this policy or applicable laws may result in legal action.

7 Vulnerability Response Matrix

Severity is determined by using CVSS scoring and internal risk evaluation.

Severity Level	Initial Acknowledgment	Triage & Assessment	Fix Deployment	Status Update Frequency
Critical	1 business day	2 business days	5 business days	Every 72 hours
High	2 business days	3 business days	10 business days	Weekly
Medium	3 business days	5 business days	20 business days	Biweekly
Low	5 business days	7 business days	As prioritized	Monthly

8 Resolution Workflow

- Acknowledgment – Confirm receipt of the report.
- Validation – Assess and verify the vulnerability.
- Risk Assessment – Assign severity level.
- Remediation – Develop, test, and deploy a fix.
- Verification – Validate fix and close the issue.
- Communication – Provide updates to the reporter (if known).

9 Exclusions

This policy does not cover:

- Physical security testing or social engineering
- Denial of Service (DoS) attacks or distributed denial of service (DDoS) attacks.
- Vulnerabilities in third-party systems that are not controlled by Subex Limited, where Subex data or operations are not directly impacted.
- Exploitation attempts causing service disruption or damage, data loss, or damage to Company systems.

Reporting Third-Party Vulnerabilities: If you discover a vulnerability in a third-party system that is used by Subex and handles Company data or provides critical services, we request that you:

- Report it to cyber.security@subex.com, detailing how it impacts Subex.
- Also, endeavor to report the vulnerability directly to the affected third party, following their disclosure policy if available.

10 Coordinated Disclosure

We require researchers to allow Subex reasonable time to fix reported vulnerabilities before disclosing them publicly. Our standard disclosure timeline is 90 days from the initial acknowledgment of a valid report, during which time public disclosure is strictly prohibited. This period may be extended by mutual agreement if the remediation is complex.
Coordinated disclosure timing and content will be discussed and agreed upon between Subex and the researcher, ideally after the vulnerability has been remediated and verified. We appreciate your cooperation in helping us protect our systems and users.

11 Recognition

While Subex does not offer monetary rewards, we appreciate the efforts of security researchers who helped us improve our security posture. For high-quality, verified reports that lead to a fix, we may offer non-monetary recognition (e.g., a mention in our "Hall of Fame" section on the Subex website), with the reporter's consent.

12 Policy Review and Enforcement

This policy will be reviewed at least annually by the Chief Information Security Officer (CISO) and updated as necessary to reflect changes in legal and regulatory requirements, industry best practices, and the Company's risk appetite. Any significant changes to this policy must be approved by Executive Leadership. The Legal Department will review and approve this policy and any significant revisions to ensure compliance.
Failure to comply with the terms of this policy, particularly regarding unauthorized access, malicious activities, or uncoordinated public disclosure, may result in disciplinary action for employees or, for external parties, the immediate withdrawal of safe harbor, pursuit of legal remedies, and/or reporting to relevant authorities.

13 Contact

For any questions regarding this policy or to submit a vulnerability report please contact cyber.security@subex.com

Updated on: 23/07/2025