Vulnerability Disclosure Policy

1. Purpose

This policy outlines considerations and commitments for the disclosure of potential security vulnerabilities to Unigen in a responsible manner.

Security Researchers

Unigen recognizes the positive contributions of security researchers and encourages the responsible and direct disclosure of potential security vulnerabilities to us. We accept vulnerability reports from all sources.

Our Commitments to Researchers

- We will maintain standard confidentiality in our communications with you
- We will work with you to validate and respond to your disclosure
- We will investigate and use all reasonable efforts to remediate validated issues in a manner consistent with protecting the safety and security of those potentially affected by a reported vulnerability
- Unigen reserves all of its legal rights in the event of noncompliance with this policy, but it does not intend to pursue legal action against any party that conducts security research and discloses information to us in good faith and as outlined in this policy
- We may offer rewards for critical or high-severity vulnerabilities based on impact and quality of submission, subject to internal review

What We Ask of Researchers

- Communicate information about potential security vulnerabilities in a responsible manner, complying with all applicable laws and respecting individual privacy
- Avoid actions that degrade user experience, disrupt systems, or destroy data
- Provide sufficient technical detail and background necessary for Unigen to identify and validate reported issues
- Act for the common good, protecting user privacy and security by refraining from publicly disclosing vulnerabilities without prior coordination

This Vulnerability Policy

- Welcomes arbitrary security research
- Includes all internet-facing assets in scope
- Provides safe harbor from CFAA and DMCA actions for all good faith research
- Does not place restrictions on disclosure when coordinated responsibly

2. Definitions

- Security Vulnerability: A weakness in a system that can be exploited to compromise the integrity, availability, or confidentiality of digital assets
- Good-Faith Researcher: An individual who makes a vulnerability disclosure without malicious intent, and avoids any privacy violation or data destruction
- Safe Harbor: Protection provided under this policy for security researchers acting in accordance with its terms

- Severity Levels:
  - Critical – Immediate business risk; full system compromise
  - High – Major impact; sensitive data exposure
  - Medium – Moderate impact; localized denial or information leakage
  - Low – Minor usability or information issues

3. Scope

Unigen defines a security vulnerability as an unintended weakness or exposure that could be used to compromise the integrity, availability, or confidentiality of our digital assets. This policy applies to all digital assets owned, operated, or maintained by Unigen, including applications, systems, public-facing websites, and our products.

In-Scope Assets

- Public-facing web applications, APIs, digital services, authentication systems
- Mobile apps, portals, cloud infrastructure endpoints owned by Unigen

Out-of-Scope Assets

- Physical social engineering (sample:, phishing, tailgating)
- Third-party platforms not managed by Unigen
- Physical hardware exploitation without written permission
- Automated vulnerability scanning without prior consent

Prohibited Behaviors Include

- Compromising the integrity, availability, or confidentiality of non-public information
- Failing to immediately delete or destroy sensitive or personal data accessed inadvertently
- Publicly disclosing any potential vulnerability without the express written consent of Unigen
- Intentionally or negligently causing denial-of-service conditions
- Exploiting vulnerabilities to send unsolicited or unauthorized messages (spam)
- Using social engineering or deceptive practices in research
- Physically connecting to networks or devices within Unigen-operated facilities
- Employees or contingent staff conducting security research outside official internal reporting channels

Researchers must contact Unigen before engaging in research that may be inconsistent with or unaddressed by this policy

4. Reporting Potential Security Vulnerabilities

If you believe you have discovered a potential security vulnerability in any digital asset owned, operated, or maintained by Unigen, or a circumstance that could reasonably impact the security of our company or our users, we encourage you to disclose this to us.

Defined Vulnerability Disclosure Process

Reports must include:

- Reporter information
- Description of the vulnerability detail
- Impact assessment
- Steps to reproduce/ data or functionality exposed

- Any supporting evidence (e.g. screenshots, logs)
- Additional notes

Researchers can report a vulnerability encrypted TLS 1.3 web page: https://unigen.com/support/vulnerability-disclosure/

Upon Submission

- We will **acknowledge receipt within 3 business days**
- We will **conduct an initial assessment within 10 business days**
- We will communicate progress, decisions, and timelines throughout the process

Reporters may request staging environment access or test credentials (if applicable) to validate remediated vulnerabilities

5. Contact and Service Level Agreement

Unigen shall use its best efforts to respond to these reported vulnerabilities according to the following:

- **Acknowledgment:** within 3 business days
- **Initial assessment**: within 10 business days
- **Remediation:** within a timeline based on severity (critical: <30 days, high: <60 days, medium < 90 days/low: as prioritized)

Escalation Path

If acknowledgment or remediation timelines are missed, researchers may escalate by sending an email, preferably using PGP encryption (e.g. Mailvelope, ProtonMail, or Virtru) with the all the questions answered from the attached file named to list of members below.

Name	Email Address	Position
Tony Bui	Tony.Bui@unigen.com	IT Manager UHAN
Ivan Lee	ivlee@unigen.com	IT Manager UHQ
Joshua Ngo	jngo@unigen.com	IT UHQ
Tuan Vu	Tuan.Vu@unigen.com	IT UHAN

Coordinated Disclosure Window: We support coordinated disclosure with a 90-days public disclosure timeline unless otherwise agreed

- **Severity-to-Remediation Mapping:**
  - Critical: < 30 days
  - High: < 60 days
  - Medium: < 90 days
  - Low: As prioritized based on impact

6. Policy Ownership and Review Cadence

- This policy is owned by Unigen

- This policy is reviewed annually or upon a significant change in threat landscape or operations.
- Next scheduled review: in 2026