



Responsible Vulnerability Disclosure Policy

Synergy Wireless Solutions

Synergy Wireless Solutions is committed to maintaining the security of our systems, services, and information. We encourage responsible, good-faith security research and appreciate reports of potential vulnerabilities that help us improve our security posture.

Reporting a Security Vulnerability

If you believe you have identified a security vulnerability related to Synergy Wireless Solutions, please report it promptly.

How to report:

- **Email:** enquire@synws.com
- **Subject:** Responsible.Disclosure.-.Security.Vulnerability

Please include, where possible:

- **A description of the vulnerability**
 - **The affected system, application, or service**
 - **Steps to reproduce the issue (if applicable)**
 - **Any relevant screenshots, logs, or supporting information**
 - **Your contact information (optional)**
-



Scope

This policy applies to:

- **Public-facing systems, applications, and services owned or operated by Synergy Wireless Solutions**
- **Corporate systems and infrastructure managed by Synergy**

This policy does not authorize testing of:

- **Systems owned or operated by customers, partners, or third parties**
 - **Physical locations, job sites, or employee devices**
 - **Systems where testing would violate applicable laws or regulations**
-

Guidelines for Responsible Research

We request that security researchers:

- **Act in good faith and avoid privacy violations**
 - **Do not access, modify, or delete data**
 - **Do not disrupt services or perform denial-of-service attacks**
 - **Limit testing to what is necessary to demonstrate the vulnerability**
 - **Do not publicly disclose vulnerabilities prior to remediation or written authorization**
-



Our Commitment

When a vulnerability is reported responsibly and in good faith, Synergy Wireless Solutions commits to:

- **Acknowledge receipt of the report within a reasonable timeframe**
- **Assess and validate the reported issue**
- **Take appropriate remediation actions based on risk**
- **Communicate status or resolution information when feasible**

Synergy will not pursue legal action against individuals who comply with this policy and act responsibly.

Disclosure and Communication

- **Vulnerability reports are handled confidentially.**
 - **Decisions regarding public disclosure are made by Synergy.**
 - **Notifications to affected parties are made when required by law or contractual obligations.**
-

No Bug Bounty

Synergy Wireless Solutions does not currently offer a bug bounty or financial rewards for vulnerability disclosures.



Legal Notice

This policy does not grant permission to:

- **Bypass authentication or authorization controls**
- **Access information beyond what is necessary to demonstrate a vulnerability**
- **Conduct testing that violates any law or regulation**

Policy Updates

This policy may be updated periodically to reflect changes in systems, services, or security practices.