# Security & Responsible Disclosure Policy

## 1.1 Our Commitment to Security

At 1factory, Inc., we take the security of our systems seriously. We are committed to protecting our users' information and maintaining the integrity of our systems. We value the security research community and welcome responsible disclosure of security vulnerabilities.

## 1.2 Reporting Security Vulnerabilities

If you discover a security vulnerability on our website or systems, we encourage you to report it to us responsibly. Please follow these guidelines:

**How to Report:**

- Email your findings to security@1factory.com
- Provide detailed information about the vulnerability, including:
    - Type and nature of vulnerability
    - Steps to reproduce the issue
    - Potential impact or risk
    - Any relevant screenshots, logs, or proof-of-concept code
    - Your contact information (individual full name and company you represent (if any)), for follow-up questions

**What to Expect:**

- We will acknowledge receipt of your report within 5 business days
- We will investigate the issue and provide updates on our progress
- We will work to validate and address confirmed vulnerabilities in a timely manner
- We will keep you informed of our remediation timeline

## 1.3 Responsible Disclosure Guidelines

To ensure the safety of our systems and users, we ask that you:

- **Do not** exploit the vulnerability beyond what is necessary to demonstrate the issue
- **Do not** access, modify, or delete data belonging to others
- **Do not** perform any action that could harm the reliability or integrity of our services
- **Do not** publicly disclose the vulnerability until we have had adequate time to address it (we request at least 90 days)
- **Do not** engage in physical attacks against our property or data centers
- **Do not** engage in social engineering attacks against our employees or users
- Act in good faith and avoid privacy violations, destruction of data, or service interruptions

## 1.4 Safe Harbor

1factory, Inc. supports responsible security research and will not pursue legal action against researchers who:

- Follow the guidelines outlined in this policy
- Act in good faith and avoid malicious intent
- Make a reasonable effort to avoid privacy violations and service disruptions
- Report vulnerabilities directly to us before disclosing them publicly

This safe harbor applies only to security research conducted in accordance with this policy.

## 1.5 Out of Scope

The following are explicitly out of scope for our disclosure policy:

- Denial of Service (DoS/DDoS) attacks
- Spamming or social engineering
- Physical attacks or attempts to gain physical access to our facilities
- Third-party websites or services linked from our website
- Vulnerabilities in third-party services we use (please report these to the respective vendors)

## 1.6 Recognition

While we do not offer a monetary bug bounty program at this time, we greatly appreciate the efforts of security researchers.

## 1.7 Questions

If you have questions about our security practices or this disclosure policy, please contact us at security@1factory.com.