APPORTO'S VULNERABILITY DISCLOSURE POLICY

Effective Date: September 4, 2025

www.apporto.com

1. Introduction

Apporto is committed to maintaining the highest standards of security for our platform and protecting our customers' data. This policy outlines our approach to handling security vulnerabilities that may affect our customers, and it details our process for vulnerability disclosure. It explains how Apporto identifies, assesses, mitigates, and communicates security vulnerabilities that could impact an organization's use of Apporto services.

2. Our Commitment

Apporto is dedicated to:

- Promptly addressing security vulnerabilities affecting our services
- Transparently communicating with our customers about security issues
- Following industry best practices for vulnerability management and disclosure
- Complying with all applicable UK data protection laws and regulations, including the UK GDPR and Data Protection Act 2018

2.1 Vulnerability Classification

Apporto classifies vulnerabilities according to the following severity levels:

Severity Level	Description
SEV 1 (Critical)	Critical security vulnerability actively exploited or easily exploitable, resulting in full system compromise, unauthorized access to sensitive data, or total service unavailability. No workaround or mitigation is available.

SEV 2 (Urgent)	Major security weakness with high likelihood of exploitation. Could lead to significant data exposure, privilege escalation, or disruption of critical functionality. No reasonable workaround is available.
SEV 3 (High)	Security vulnerability that affects some systems, users, or components. Exploitation would have moderate impact (e.g., partial data exposure, limited privilege escalation). Temporary or partial workaround exists but is not scalable.
SEV 4 (Medium)	Security misconfiguration or lower-risk vulnerability with limited impact, affecting a small number of users or systems. Exploitation is difficult or requires unusual conditions. A reasonable workaround or mitigation is available.

2.2 Response Timeline

Apporto adheres to the following target response and resolution times, designed to meet the most restrictive regulatory requirements across UK, EU, and US jurisdictions:

Severity Level	Initial Response	Target Resolution	Regulatory Notification
SEV 1 (Critical)	1 hour	8 hours	Authorities: 24 hours Customers: 72 hours max
SEV 2 (Urgent)	2 hours	24 hours	Authorities: 24 hours Customers: 72 hours max
SEV 3 (High)	4 business hours	48 business hours	As required by regulation
SEV 4 (Medium)	8 business hours	As soon as practicable	As required by regulation

Note: For any vulnerability involving personal data or constituting a security breach under applicable data protection laws, Apportowill notify relevant authorities within 24 hours and affected individuals within 72 hours maximum, regardless of SEV level.

3. Notification Process

When Apporto becomes aware of a security vulnerability that could impact our customers, Apporto follows a comprehensive notification process that meets the most restrictive requirements across UK, EU, and US regulations:

3.1 Immediate Actions (0-24 hours)

1. **Initial Assessment**: Our security team conducts an immediate assessment to determine severity, scope, and potential impact
2. **Regulatory Notification**: For any incident involving personal data or qualifying as a security breach, Apporto will notify relevant authorities within 24 hours:
    - UK: Information Commissioner's Office (ICO) and relevant NIS authorities
    - EU: Relevant Data Protection Authorities in affected member states
    - US: State attorneys general and other authorities as required by applicable state laws

3.2 Customer Notification (24-72 hours)

3. **Customer Communication**: For vulnerabilities classified as SEV 1 or SEV2, or any incident involving personal data with high risk to individuals, Apporto will notify affected customers within 72 hours maximum
4. **Risk-Based Notification**: For lower severity vulnerabilities, notification timing is determined by risk assessment but always within regulatory requirements

Ongoing Management

5. **Regular Updates**: Continuous communication on remediation progress
6. **Resolution Notice**: Final notification upon vulnerability resolution with complete details

3.3 Multi-Jurisdictional Considerations

- Apporto maintains a Compliance Lead familiar with UK, EU, and US requirements
- All notifications are crafted to meet the content requirements of the most restrictive applicable regulation
- Apporto coordinates with legal counsel in each jurisdiction as needed

4. Notification Methods

Apporto will use multiple notification methods to ensure compliance with the most restrictive requirements across all applicable jurisdictions:

4.1 Primary Notification Methods (Used for All Significant Breaches)

- **Direct Written Communication**: Email to the organization's designated security and data protection contacts (required by most US state laws)
- **Registered Mail**: For critical incidents where required by applicable law (US state law compliance)

4.2 Secondary Notification Methods

- **Apporto Admin Portal**: Security notifications posted to the administrator dashboard with read-receipt tracking
- **Status Page**: Updates on our service status page at https://www.apporto.com/status
- **Security Bulletins**: Formal security bulletins for critical vulnerabilities

4.3 Public Notification (When Required)

- **Website Notice**: Prominently displayed on our main website when required by regulation
- **Media Notice**: Publication in major newspapers or media outlets when required by US state laws for large-scale breaches
- **Regulatory Filings**: SEC or other regulatory filings as required by applicable law

4.4 Multi-Language Support

For our global customer base, critical notifications will be provided in English, and other languages as required by local regulations or customer agreements.

5. Information Provided

When notifying the customer of a vulnerability, Apporto will include comprehensive information that meets the disclosure requirements of UK GDPR, EU GDPR, and US state breach notification laws. The information provided will include the most detailed requirements from any applicable regulation:

5.1 Required Information (Per Most Restrictive Standards)

- **Nature of the vulnerability** and security breach (required by all jurisdictions)
- **Categories and approximate number of data subjects/individuals concerned** (GDPR requirement, adopted for all notifications)
- **Categories and approximate number of data records affected** (GDPR requirement, adopted for all notifications)
- **Likely consequences** of the security breach (GDPR requirement, adopted for all notifications)
- **Measures taken or proposed to address the breach** including measures to mitigate adverse effects (GDPR requirement, adopted for all notifications)
- **Contact details** of our Data Protection Lead and security team (GDPR requirement, adopted for all notifications)
- **Severity classification** using our SEV system
- **Systems or services affected**
- **Timeline of the incident** (enhanced US state law requirement, adopted for all notifications)
- **Temporary workarounds or mitigations** (if available)
- **Steps Apporto is taking to address the issue**
- **Estimated timeline for resolution**
- **Specific steps the customer should take** to protect data and mitigate risks
- **Reference to any public CVE** (Common Vulnerabilities and Exposures) identifier if applicable

6. Customer Responsibilities

To ensure effective communication regarding security vulnerabilities, Apporto asks that the customer:

- Keep security contact information current by submitting a Support ticket to Apporto anytime customer security contact changes occur
- Acknowledge receipt of vulnerability notifications
- Implement any recommended mitigations in a timely manner
- Maintain confidentiality of vulnerability information as requested
- Notify us of any questions or concerns about our remediation efforts

7. Confidentiality

Apporto treats vulnerability information with strict confidentiality and expects the same from our customers. For certain high-severity vulnerabilities, Apporto may request that customers maintain confidentiality until a fix has been deployed to all affected customers.

8. Responsible Disclosure

Apporto practices responsible disclosure and will not publicly disclose vulnerabilities until:

- A fix or mitigation has been developed and tested
- The fix has been applied to all affected systems, or
- Affected customers have been notified and given reasonable time to implement mitigations

9. Continuous Improvement

Following any significant security incident, Apporto conducts a thorough post-mortem review to identify lessons learned and improve our security processes. Apporto may share anonymized findings with customers to help strengthen the security posture of our entire user base.

10. Regular Security Assessments

Apporto conducts regular security assessments, including:

- Vulnerability scanning
- Penetration testing
- Code reviews
- Third-party security audits

A summary of these assessments can be provided to customers upon request, subject to appropriate confidentiality agreements.

11. Legal and Regulatory Compliance

This policy has been developed to meet the most restrictive requirements across multiple jurisdictions and regulatory frameworks to ensure comprehensive compliance:

11.1 UK Regulations

- **UK GDPR and Data Protection Act 2018**: Personal data breach notifications within 72 hours to the ICO, and without undue delay to affected data subjects when high risk is identified
- **NIS Regulations 2018**: Notification of significant cybersecurity incidents to relevant authorities within 24 hours for essential service providers
- **NCSC guidance**: Following National Cyber Security Centre best practices for vulnerability disclosure and incident management

11.2 EU GDPR Requirements

- **Article 33**: Notification to supervisory authorities within 72 hours of becoming aware of a personal data breach
- **Article 34**: Communication to data subjects without undue delay when breach is likely to result in high risk to rights and freedoms
- **Article 32**: Implementation of appropriate technical and organizational measures to ensure security of processing

11.3 US Regulatory Framework

- **State Data Breach Notification Laws**: Compliance with the most restrictive state requirements, including California's SB-1386 and other state laws requiring notification without unreasonable delay
- **NIST Cybersecurity Framework**: Adherence to NIST guidelines for incident response and vulnerability management
- **Sector-specific requirements**: Including HIPAA (where applicable), SOX, and other relevant federal regulations

12. Apporto’s Unified Approach

To ensure compliance across all jurisdictions, Apporto applies the most restrictive standard from the above frameworks:

- **Personal Data Breach Notification**: Apportowill notify relevant authorities within **24 hours** (the most restrictive of UK NIS, EU GDPR 72-hour, and varying US state requirements)
- **Customer/Data Subject Notification**: Affected individuals will be notified **without undue delay and within 72 hours maximum** for high-risk breaches
- **Documentation**: All incidents will be documented in accordance with the highest standard required by any applicable regulation
- **Risk Assessment**: Apporto conducts comprehensive risk assessments using the most stringent criteria from all applicable frameworks

13. Contact Information

For questions about this policy or to report security concerns, please contact:

Apporto Security Team
Email: security@apporto.com

Document Review / Revision History

Date	Version	Action / Change	Reviewed / Approved By:
09.03.202	1.1		
08.26.2025	1.1	Updated wording and formatting	Nahum Nicholas
05.29.2025	1.0	Policy release	Travis Markley

Effective Date: 08.26.2025
Review Cadence: At least annually
Other triggering events set out herein
Next Scheduled Review: 08.27.2026