RANDOX

Vulnerabilities and Incident Handling Policy

1. Our Commitment to Cyber Security

At Randox, we are committed to maintaining the highest standards of cybersecurity to protect our clients, their customers, and our systems.

To achieve this, we implement a multi-layered security approach, including:

- **Security by Design:** We keep a close eye on any vulnerabilities, incidents, and other cybersecurity threats to ensure our products remain secure throughout their entire lifecycle. By doing this, we aim to provide timely security updates that minimize any disruption to how our products are used, ensuring they remain safe, effective, and reliable. We also strive to protect the availability and integrity of the data associated with our products.

- **Independent security assessments:** We conduct regular penetration testing with CREST-approved vendors to identify and mitigate security risks proactively.

- **Continuous monitoring:** Our security operations include real-time threat detection and automated vulnerability scanning to detect potential issues before they become threats.

- **Adherence to best practices and compliance frameworks:** We follow industry-leading security standards, such as ISO 27001 and NIST CSF.

Security is a shared responsibility, and we encourage our clients to report any security Vulnerabilities or security incidents relating to our products identified/notified to by their customers so that we can investigate and resolve them promptly.

2. Scope of this policy

This policy only applies to the security vulnerabilities and security incidents relating to publicly or internally accessible devices, systems, applications, cloud hosted services, APIs owned or operated by Randox at our client locations.

2.1 Out of Scope

All other systems, devices, infrastructure and services belonging to Randox including but not limited to:

- Third party services – Integrated in our platform
- Social engineering attacks, such as Phishing or impersonation of employees
- Physical security vulnerabilities
- Denial of Services attacks or any actions that disrupt the availability of services.
- Publicly accessible sites of Randox, Infrastructure, Cloud hosted apps and services, etc.

3. Our Definition of a Security vulnerability

Randox will define security vulnerability as a gap, defect, or improper setup in a system, software, or network that can be taken advantage of to undermine its confidentiality, integrity, or availability.

3.1 Categories of Security vulnerabilities

Security vulnerabilities can take various forms, including but not limited to:

Application Security Flaws

- Injection attacks: SQL injection, command injection, LDAP injection.
- Cross-Site Scripting (XSS): Stored, reflected, or DOM-based attacks that allow attackers to inject malicious scripts.
- Cross-Site Request Forgery (CSRF): Trick users into performing unintended actions.
- Broken access controls: Privilege escalation, unrestricted API access, improper role-based access control (RBAC).
- Authentication vulnerabilities: Weak password policies, lack of multi-factor authentication (MFA), session hijacking.

Infrastructure & Network Security Issues

- Insecure server configurations: Open ports, exposed services, misconfigured cloud storage (e.g., open S3 buckets).
- Sensitive data exposure: Unencrypted storage or transmission of sensitive data, hardcoded credentials.
- Server-Side Request Forgery (SSRF): Exploiting misconfigured services to send unauthorized requests.
- Remote Code Execution (RCE): Allowing attackers to execute arbitrary commands on a system.

Supply Chain & API Security Risks

- Insecure APIs: Missing authentication, exposed data, lack of rate limiting.
- Third-party dependencies: Outdated or vulnerable components.
- Weak encryption or hashing algorithms: Use of deprecated cryptographic protocols.

If a security issue does not fall into these categories but poses a potential risk, we encourage responsible reporting.

4. Reporting a security vulnerability/incident

If you are our client and have identified a potential vulnerability/or have been notified of a potential vulnerability by any of your customers relating to assets mentioned within the Scope Section of this document, we would request you notify us immediately.

4.1 How to report a security vulnerability/incident

To ensure a swift response, please send a security report to our security team via email: securityissue@randox.com

Your report should include as much detail as possible, including:

- **A clear description of the reported issue:** What was observed, how it was discovered, and any known impact.
- **The affected system, service, or feature:** URLs, application versions, or API endpoints (if applicable).
- **Steps to reproduce the vulnerability:** Proof-of-concept code, screenshots, logs, or any supporting evidence.
- **Date and time of the initial report:** When the issue was first reported to you by your customer.
- **Any additional details that may assist in remediation:** Suggested mitigations, affected user groups, etc.

4.2 What to expect from us

Once we receive your report aligned with Section 4.1 of this document, we commit to the following process:

- **Acknowledgment** – We will confirm receipt of your report within [X] business days.
- **Investigation & Assessment** – Our security team will analyse the issue, verify its impact, and prioritize remediation based on severity.
- **Communication & Updates** – We will provide regular updates on the status of our investigation and mitigation efforts.
- **Resolution & Remediation** – If the vulnerability is confirmed, we will deploy fixes or mitigations and notify affected parties.

5. Responsible Disclosure Guidelines

We encourage responsible disclosure to ensure vulnerabilities are handled safely. We request that:

- Security vulnerabilities are reported directly to us before public disclosure.
- No unauthorized testing is conducted beyond what is necessary to report an issue.
- No attempts are made to exploit, manipulate, or retain access to any sensitive data.
- Clients work with us in a cooperative manner to mitigate risks.
- No unauthorized testing of Randox infrastructure or assets that maybe out of scope for this policy – refer section 2 Scope of Policy for more details.
- Do not include any sensitive information including and not limited to PII, PHI, financial information or patient information in the reports.

6. Compliance with Laws and Regulations

Our security and vulnerability management practices align with applicable cybersecurity laws and regulatory requirements, including but not limited to:

Data Protection & Privacy Laws

- General Data Protection Regulation (GDPR) (EU/UK) – Ensures the protection of personal data and requires organizations to address security vulnerabilities to prevent data breaches.
- UK Data Protection Act 2018 – Provides additional data protection regulations aligned with GDPR in the UK.
- California Consumer Privacy Act (CCPA) – Requires businesses to safeguard consumer data and disclose breaches.

Cybersecurity Frameworks & Regulations

- ISO 27001 – International standard for information security management, requiring proactive risk management and vulnerability remediation.
- NIST Cybersecurity Framework (NIST CSF) – Provides best practices for identifying, protecting, detecting, responding to, and recovering from cybersecurity threats.
- Cyber Assessment Framework (CAF) – Used for assessing cybersecurity readiness and resilience in critical sectors.

Failure to comply with applicable security regulations can result in legal consequences, financial penalties, and reputational damage. We take security compliance seriously and continuously adapt to evolving regulatory requirements.