Security Policy

Last updated: 2026-06-12

This Security Policy is part of our Privacy Policy and details our commitment to protecting your data. For information about data transfers and processing, please refer to our Data Transfer Policy and Data Collection & Processing Policy (www.andri.ai/legal).

1. ANDRI AUDITS AND CERTIFICATIONS

1.1. The information security management system used to provide the Service will be assessed by independent third-party auditors and through self-declared compliance as described in the following: ISO 27001 certified by Kiwa (certificate number K-0229199/1, verifiable via the Kiwa certificate finder at kiwa.com).

1.2. Third-Party Audit reports and compliance documentation are made available to You as described in Section 10.1.

1.3. To the extent that Andri decides to discontinue any certification or compliance program, Andri will adopt an equivalent, industry-recognized framework.

2. HOSTING LOCATION OF CUSTOMER DATA AND CONTENT

2.1. Customer Data and Content will be stored and processed by Andri and its vendors in data centers located in the European Economic Area (EEA) or the United Kingdom, as specified in our Data Transfer Policy.

2.2. You may request to have Your Customer Data and Content stored in a specific geographic region. Andri will use commercially reasonable efforts to accommodate such requests where supported by our cloud service provider(s) and compliant with applicable EU and UK laws, including GDPR.

3. ENCRYPTION

3.1. Andri encrypts Customer Data and Content at rest using AES 256-bit encryption or better. Andri uses Transport Layer Security (TLS) 1.2 or better for data in transit over public or untrusted networks.

3.2. Encryption keys are rotated at least annually, safeguarded with hardware security modules, and logically separated from Customer Data and Content.

4. SYSTEM AND NETWORK SECURITY

4.1. Access Control: Andri personnel access the Cloud Environment with unique user IDs, adhering to the principle of least privilege, and requiring multi-factor authentication and secure connections.

4.2. Restricted Access: Andri personnel will not access Customer Data or Content except (i) to provide or support the Service, or (ii) to comply with applicable laws or binding legal orders as detailed in our Privacy Policy.

4.3. Device Security: Company-issued laptops used to access the Cloud Environment are encrypted, monitored with endpoint detection and response tools, and kept up to date with vulnerability patches.

4.4. Threat Detection: The Cloud Environment uses industry-standard tools to detect and alert for suspicious activities, including malware and malicious code.

4.5. Penetration Testing: Independent third parties conduct annual penetration tests. Summary results are available upon request (Section 10.1).

4.6. Vulnerability Management: Vulnerabilities are prioritized and resolved within timelines aligned with their criticality (e.g., critical: 7 days; high: 30 days; medium: 90 days).

4.7. Application Security Testing: Andri engages independent security assessments annually, testing against vulnerabilities such as OWASP standards.

5. ADMINISTRATIVE CONTROLS

5.1. Security Training: All personnel receive security awareness training upon onboarding and annually thereafter. This includes GDPR compliance, secure development practices, and phishing prevention.

5.2. Secure Development: Developers receive annual training on secure coding practices, covering topics like threat modeling, authentication bypass prevention, and secure design principles.

5.3. Confidentiality Agreements: Personnel sign confidentiality agreements and acknowledge their responsibilities for reporting security incidents.

5.4. Access Review: Critical system access is removed within one day of separation, with all system access removed within three days. Privileged accounts are reviewed quarterly.

5.5. Background Checks: Personnel with access to Customer Data undergo identity verification, right-to-work checks, and criminal history screening, where

legally permitted.

6. VENDORS AND SUB-PROCESSORS

6.1. Vendors that process Customer Data are required to maintain security measures consistent with Andri's obligations under this Security Addendum.

6.2. A complete list of sub-processors is maintained at www.andri.ai/legal/subprocessors.

7. PHYSICAL DATA CENTER CONTROLS

7.1. Andri's cloud providers maintain physical security controls audited under ISO 27001 and SOC 2 Type II. These include: controlled facility access, visitor ID requirements, access control devices, and fire detection, climate control, and redundancy systems.

7.2. No Customer Data is stored at Andri's corporate offices.

8. INCIDENT DETECTION AND RESPONSE

8.1. Incident Notification: In the event of a breach involving Customer Data, Andri will notify You without undue delay, where possible within 24 hours and no later than within 72 hours of becoming aware, in line with our data processing agreement and as detailed in our Data Collection & Processing Policy.

8.2. Incident Handling: Andri will take reasonable steps to contain and investigate the incident. Logs relevant to an incident are preserved for the duration of the investigation and any follow-up obligations.

8.3. Incident Communication: Timely updates will be provided regarding the nature of the breach, its impact, and mitigation steps.

9. AUDIT LOGGING

9.1. Audit logs of system activity are maintained for a minimum of 90 days, in accordance with our Logging and Monitoring Policy, to support monitoring and investigation.

9.2. Logs are protected from tampering.

10. CUSTOMER AUDIT RIGHTS

10.1. Upon request, Andri will provide access to: the ISO 27001 certification (certified by Kiwa) and penetration test summaries.

10.2. Customers may submit annual security questionnaires and receive responses at no additional cost.

10.3. In the event of a security incident, Andri will provide forensic analysis results to impacted customers.

11. CUSTOMER RESPONSIBILITIES

11.1. Ensure lawful usage of Customer Data with the Service, including compliance with GDPR and other applicable laws as outlined in our Acceptable Use Policy.

11.2. Maintain security of access credentials and report suspected breaches promptly.

11.3. Keep systems used to access the Service updated and patched.

12. BUSINESS CONTINUITY AND DISASTER RECOVERY

12.1. Andri maintains business continuity plans reviewed and tested annually, covering contingencies for processes, systems, and partnerships. For more details about our service commitments, please refer to our Support & Service Level Agreement.