

Nimbleford Analytics, Inc.

Responses to the customer's vendor security questionnaire for the Nimbleford Insights platform. Supporting documentation, including our SOC 2 Type II report, is available under NDA.

ID	Question · answer and vendor notes
Audit & Assurance	
A&A-01	Do you have a current SOC 2 Type II report? State the auditor and period. YesSOC 2 Type II, issued by Quillfeather & Rook LLP for October 1, 2025 to September 30, 2026.
A&A-02	Which Trust Services Criteria are in scope? YesSecurity, Availability and Confidentiality.
A&A-03	Did your most recent audit report any exceptions or deviations? NoNo exceptions were noted in our latest SOC 2 report.
A&A-04	Does the audit scope cover all infrastructure used to deliver the service? YesAll production infrastructure is covered by our SOC 2 report, including hosting.
A&A-05	Do you hold ISO/IEC 27001 certification? YesWe are ISO/IEC 27001 certified.
Identity & Access Management	
IAM-01	Is multi-factor authentication required for workforce access to production? YesMFA is enforced for all workforce accounts through our SSO identity provider.
IAM-02	Is privileged access to production databases restricted? YesDatabase access is just-in-time, limited to the infrastructure team and on-call engineers, for a maximum of eight hours.
IAM-03	Are user access rights to production reviewed periodically? YesQuarterly access reviews are completed by system owners within 15 days of every quarter end.
IAM-04	How quickly is access removed when personnel leave? YesAccess is revoked within one business day of termination for all employees and contractors.
IAM-05	Are customers required to manage any access controls themselves? NoNimbleford manages all access to the platform on the customer's behalf.
Cryptography & Key Management	
CEK-01	Is customer data encrypted at rest? State the algorithm. YesAES-256 at rest.

ID	Question · answer and vendor notes
CEK-02	Is customer data encrypted in transit? Yes TLS 1.2 or higher for all connections.
Data Security & Privacy	
DSP-01	Where is customer data stored? Yes Customer data is stored only in the United States (AWS US East, with backups in US West).
DSP-02	How is customer data segregated in the multi-tenant platform? Yes Each tenant is isolated with row-level security keyed to a tenant ID, verified by automated tests.
DSP-03	How long after contract termination is customer data deleted? Yes Deleted from production systems within 30 days of termination.
Change Control	
CCC-01	Are all production changes peer reviewed before deployment? Yes Every production change requires approval by a second engineer; branch protection enforces this.
Threat & Vulnerability Management	
TVM-01	How often do you scan for vulnerabilities? Yes Authenticated scans weekly; critical issues fixed within 15 days, high within 30 days.
TVM-02	Do you conduct annual third-party penetration testing? Summarize the latest results. Yes Annual third-party penetration test (May 2026). No high or critical findings.
TVM-03	Do you operate a bug bounty program? No No paid program; researchers report issues under our responsible disclosure policy.
Logging & Monitoring	
LOG-01	How long are security logs retained? Yes Logs are retained for 12 months in our SIEM.
Security Incident Management	
SEF-01	Do you have an incident response plan, and is it tested? Yes Yes; tested annually by tabletop exercise (most recent April 14, 2026).
SEF-02	Within what timeframe will you notify customers of a security incident affecting their data? Yes Within 72 hours of confirming the incident.
Business Continuity & Resilience	
BCR-01	How frequently are backups taken, and how long are they retained? Yes Daily backups, encrypted and replicated to a second region, retained for 35 days.

ID	Question · answer and vendor notes
BCR-02	State your recovery point objective (RPO) and recovery time objective (RTO). Yes RPO of 1 hour and RTO of 4 hours.
BCR-03	Is the disaster recovery plan tested? Yes Tested annually; the last full test was March 9, 2026.
BCR-04	What availability do you commit to? Yes 99.9% monthly uptime, excluding scheduled maintenance.
Human Resources	
HRS-01	Are background checks performed on new employees? Yes Background checks are completed before every new hire's start date.
HRS-02	Do personnel complete security awareness training? Yes At hire and annually for all personnel.
Supply Chain & Third Parties	
STA-01	Do you assess your own critical suppliers? Yes Vendors are assessed before engagement and reviewed annually, including their SOC 2 reports.
Governance & Risk	
GRC-01	Do you carry cyber liability insurance? State the limit. Yes Cyber liability coverage with a \$10 million limit.

The Security team attests that these responses are accurate to the best of its knowledge as of the date above.