DashboardFox Security Overview

5000fish, Inc. | September 2026 | dashboardfox.com/security/review-kit/

This overview describes the security program for the DashboardFox cloud-hosted service, operated by 5000fish, Inc. It is organized in the order most vendor security questionnaires follow. Supporting documents are listed at the end and are available on request, under NDA where appropriate.

Service and deployment model

- DashboardFox is cloud-hosted business intelligence and reporting software, delivered as SaaS. A self-hosted edition is also available and runs entirely on the customer's infrastructure.
- Standard deployment is multi-tenant. Each customer workspace runs in its own isolated database with unique credentials and workspace-scoped authorization. There is no shared application data path between tenants.
- Enterprise Dedicated Cloud is a single-tenant deployment: a dedicated server and a dedicated PostgreSQL database that serve one customer, with separate production and development workspaces available.
- Customers choose a US or EU data region. Data stays in that region.

Hosting and sub-processors

- Infrastructure is hosted with OVHcloud in separate US and EU regions. The US region is a HIPAA/HITECH-attested facility.
- Encrypted backups are stored offsite with Backblaze B2, in the same region as the customer. DNS is provided by Cloudflare. Operational logging uses Axiom.
- Providers that store customer data are covered by executed BAAs or DPAs before any regulated data is provisioned. We confirm confidentiality, security, breach-notification, residency, and return-or-destruction clauses before engaging a provider.
- The full sub-processor registry is published and kept current.

How customer data is handled

- Source data remains in the customer's own database. DashboardFox queries it on demand with read-only access and does not require the data to be copied into the platform.
- Report definitions, metadata, and any data a customer chooses to import are held in that customer's own encrypted database.
- Operational logs are configured to exclude PHI and customer report data.
- No AI or machine-learning model processes customer data, and no customer data is shared with any third-party AI provider. AI features are on the product roadmap and are governed by an AI Risk Management Policy aligned to the NIST AI RMF. We do not train on customer data.

Encryption and secrets

- At rest: AES-256 transparent data encryption on all databases.
- In transit: TLS 1.2 or higher on all connections.
- Backups are encrypted on the server before they leave it. The decryption key is held offline by 5000fish.
- Database credentials, API keys, and tokens are stored in encrypted secrets management, never in plaintext or source code.
- Outbound email such as scheduled reports can be sent through the customer's own SMTP gateway, so customer email is not relayed through shared infrastructure.

Workforce access

- Production access follows least privilege and is limited to a small number of named personnel. There are no contractors with access to customer data.
- Host access is by SSH key only, with password login disabled, to hardened hosts protected by a firewall and automated intrusion prevention.
- Elevated application access is just-in-time: retrieving the credential requires a documented reason that is written to the audit log, and the credential is rotated after each use.
- Background checks are completed before employment. Access is reviewed at least annually, and access is revoked with credentials rotated on separation.
- Workforce credentials are unique, held in a password manager, and protected by MFA wherever supported.

Authentication and authorization in the product

- Password security is permanently enabled on DashboardFox Cloud and follows NIST SP 800-63B: a 12-character minimum, screening against common and publicly breached passwords, and account lockout after five consecutive failed attempts. Breach screening uses k-anonymity, so passwords are never transmitted.
- Management portal: multi-factor authentication by authenticator app or SMS code, with session controls and token expiry. SSO with SAML or OIDC identity providers is supported for the admin console through an identity-aware proxy.
- End-user login: configurable password and session policies, with multi-factor authentication available through Cisco Duo.
- In development: native Enterprise SSO (SAML 2.0 and OIDC) for end users, native two-factor authentication, forced password change with administrator lock-out and disable, and self-service password reset.
- Authorization: role-based access control with row-level and field-level security on reports, dashboards, and data sources, plus IP restrictions and concurrent-session control. These controls are included on every plan.

Logging, monitoring, and audit

- Operating-system, SSH authentication, and container logs are shipped in real time to a centralized log platform with alerting and saved monitoring queries. Host-level audit rules watch sensitive files such as the encryption keyring.
- The in-app audit trail records report executions, logins, permission changes, data-source access, exports, and prints. It is stored in the customer's own DashboardFox database and the customer can query it directly. 5000fish does not ingest customer activity logs into its own systems.
- Workspace audit logs are retained by plan, up to 365 days. Database audit logs are retained for six years where required, which meets HIPAA's record-retention requirement for BAA customers.
- Administrative actions in the management portal are logged separately. Availability is published on a public status page.

Security testing and vulnerability management

- Continuous automated penetration testing by an independent third-party provider, grey-box, with weekly reports. Testing covers the OWASP Top 10, including cross-tenant access control.
- Full results are shared with customers and prospects under NDA. Independent manual penetration testing is under evaluation.
- A Vulnerability Disclosure Policy is published, with an initial response within 5 business days and an assessment within 14 business days.
- Operating-system security patches are applied automatically. Major and emergency changes receive manual review, and critical fixes are handled as emergency maintenance.

Change management and secure development

- Every change goes through pull-request review with a distinct author and approver, and is tracked to a ticket.
- Development and production environments are separated. Secrets are never committed to code. Dependencies are updated through the same change process.
- A master change log is maintained for production systems, and a trailing six-month summary is available on request.

Incident response and breach notification

- A documented Incident Response Plan covers preparation, detection, analysis, containment, eradication and recovery, and post-incident review, with named roles and incidents tracked to closure.
- Incidents are acknowledged within 1 hour of detection, with updates every 2 hours while an incident is active, as set out in the published SLA.
- Personal-data breaches are notified within 72 hours of confirmation under GDPR and UK GDPR. Where PHI is involved, covered-entity customers are notified under the executed BAA and HIPAA.

Business continuity and disaster recovery

- Recovery is a rebuild-from-code process using infrastructure-as-code, combined with restore from encrypted offsite backups.
- Backups run nightly, so the recovery point is bounded by the nightly cycle. Daily backups are kept for 90 days and weekly snapshots for 13 months.
- Backup restoration and decryption are tested every six months, with results and corrective actions recorded.
- Documented runbooks and centralized monitoring support continuity. Recovery objectives are reviewed with customers during their security review.
- The service carries a 99.5% monthly uptime commitment, with 48 hours' notice of disruptive maintenance.

Physical and endpoint security

- 5000fish is a fully remote company with no office or data center of its own. Physical security for production is inherited from the hosting provider, whose attestations are available on request. No 5000fish personnel require physical data-center access.
- Workstations use full-disk encryption, automatic screen lock, automatic updates, a host firewall, and built-in anti-malware. Server and workstation hardening standards are documented.

Compliance and insurance

- HIPAA: a Business Associate Agreement is available on Enterprise Dedicated Cloud with the Compliance Tier. Sub-processor BAAs are executed before any PHI is provisioned.
- For HIPAA business-associate work, 5000fish maintains a standalone $5M cyber liability policy and raised E&O and general liability limits.
- GDPR and UK GDPR: Data Processing Agreement with EU or US data residency. CCPA-aligned data handling. A FERPA Education Data Addendum is available on any paid plan.
- SOC 2 Type II is on our roadmap. Controls were designed to the SOC 2 criteria, and the program is documented in a policy set of 18 policies with a traceability matrix that maps each control to standard questionnaire items.

Documents available on request

Provided to customers and prospects during a security review, under NDA where appropriate.

- Security Overview (this document)
- Response and Evidence Traceability Matrix
- Enterprise Risk Management Policy
- Vendor and Sub-processor Management Policy
- Information Security Policy and System Security Plan
- HR and Personnel Security Policy

- Policy Acknowledgement and Constituent List
- Physical Access and Facility Security Policy
- Change Management Policy
- System Maintenance and Patch Management Policy
- Logging and Monitoring Policy
- Access Control and Account Management Policy
- Secure SDLC Policy
- Incident Response Plan
- Business Continuity and Disaster Recovery Plan
- Endpoint Configuration and Hardening Standard
- Network Security Policy, with network diagram
- Data Classification, Inventory and Flow Policy, with data-flow diagram
- AI Risk Management Policy
- Latest penetration test report
- Business Associate Agreement and Data Processing Agreement
- Certificate of insurance

Contact

Security reviews and document requests: team@dashboardfox.com, or dashboardfox.com/contact/?topic=security-review. Questionnaires are completed directly by the engineers who operate the service.