Logging & Monitoring Policy

1. Purpose

This policy sets out what Subcontext logs, how long logs are kept, how they are protected and how they are monitored. Good logging lets Subcontext detect and investigate security incidents and faults, show customers and regulators what happened and who did it, and keep the platform available. Logs can themselves contain personal data, so this policy also makes sure they are kept only as long as needed and protected like the data they describe.

2. Scope

This policy covers:

- The Subcontext platform in production: the web application, background workers, database, cache, file storage, load balancer, web application firewall and network
- Logs and records kept by the application, including the audit log and compliance decision trail
- Infrastructure logs and alarms in AWS
- Error monitoring and performance monitoring

3. Definitions

Term	Meaning
Log	A time-stamped record of an event in a system
Audit log	The application's record of significant user and administrator actions, used for accountability
Compliance decision trail	The tamper-evident record of compliance decisions about AI agents' actions
Alert	A notification sent to people when a monitored condition is met
Security event	An observable occurrence that may affect security, such as repeated failed sign-ins or blocked attacks

4. What Is Logged

Log	Contents	Kept for
Audit log	Significant user and administrator actions: who, what, when, from where, and on whose behalf when an administrator is acting for a customer	2 years
Compliance decision trail	Every compliance decision about an AI agent's actions, hash-chained and sealed every minute so tampering is detectable	6 years by default, configurable per customer

Log	Contents	Kept for
Application logs	Requests and application events	30 days
Network flow logs	Network traffic metadata	30 days
Web application firewall logs	Blocked and rate-limited requests	30 days
Load balancer access logs	Requests reaching the platform	Retained in encrypted storage
Database logs	Database events and errors	Retained in CloudWatch
Integration request logs	Calls to and from customers' connected systems	90 days
API request logs	Calls to the Subcontext API	3 months
AI model call logs	Calls to AI models, for cost and quality monitoring	13 months
Error reports	Application errors	90 days
Performance data	Request timings	10 days

4.1 Audit log detail

The audit log covers around 330 types of event across the platform, such as changes to users, settings and integrations. Each entry records:

- Who acted, and the Subcontext administrator acting on their behalf where an administrator is impersonating a user
- What was done, and to which record
- When it happened
- The IP address, browser (user agent) and request it came from

When a Subcontext administrator starts or stops impersonating a customer's user, that is itself recorded, and every action taken while impersonating records the administrator.

4.2 Compliance decision trail detail

- The trail is kept for 6 years by default, and customers can set a period between 3 and 25 years
- Entries are hash-chained, so each entry depends on the one before it, and the chain is sealed every minute
- The trail refuses to be purged if its hash chain has been broken

4.3 What must not be logged

The following must never be written to logs in readable form:

- Passwords, one-time codes and backup codes
- Access tokens, API keys, session identifiers and other secrets
- Card details, which Subcontext never receives, and Direct Debit bank details
- Values given to AI agent tools that are marked sensitive

5. Protecting Logs

- Audit log entries cannot be altered once written
- The compliance trail refuses to be purged if its hash chain has been broken
- Passwords, tokens, one-time codes and other sensitive values are filtered out of logs
- Sensitive values given to AI agent tools are recorded as redacted
- Access to logs is limited to the people who need it

In addition:

- Logs are classified as Confidential under the Data Classification Policy, because they can contain personal data
- Infrastructure logs are held in AWS, which is accessed only by named members of the team
- Customers see the audit log for their own organisation only
- Logs are deleted automatically when their retention period ends, in line with the Data Retention & Deletion Policy

6. Monitoring and Alerting

- Application errors alert the engineering team by email the first time they occur, if they recur after being resolved, and as their count grows
- Infrastructure alarms cover the database, cache, load balancer and application servers
- The web application firewall blocks known-bad traffic and rate-limits abusive clients automatically
- A daily heartbeat message to the team confirms that scheduled processing is running
- Health checks remove unhealthy application servers automatically

6.1 Monitoring in detail

Area	What is monitored	How alerts reach people
Application errors	Errors in web requests and background jobs	Email to the engineering team
Infrastructure	Database, cache, load balancer and application server alarms	Email to hello@subcontext.com
Attacks and abuse	Requests blocked by the web application firewall's managed rule sets (common exploits, SQL injection, known bad inputs, IP reputation, Linux and Unix attacks) and its per-IP rate limit; application rate limits on sign-in and other features	Blocked automatically; firewall logs kept for 30 days
Account security	An account is locked for 10 minutes after 3 failed sign-in attempts	Locked automatically
Scheduled processing	The daily heartbeat message to the team	A missing heartbeat is noticed by the team and investigated
Availability	Health checks on application servers	Unhealthy servers are replaced automatically

6.2 Areas for development

At each review of this policy, Subcontext will consider whether to add a cloud-wide audit trail of infrastructure changes and a managed threat detection service, taking account of the growth of the platform and customers' assurance needs.

7. Responding to Alerts

1. The person receiving the alert acknowledges it and checks whether it is genuine
2. Faults are fixed and the error is resolved in the error monitoring tool, so that a recurrence alerts again
3. Anything that may indicate a security incident, such as unexpected administrator activity, a spike in blocked requests or signs of unauthorised access, is handled under the Incident Response Plan
4. Where logs are needed as evidence, the relevant entries are preserved before their retention period ends

8. Roles and Responsibilities

Role	Responsibility
Security Officer	Owns this policy, reviews administrator activity, and checks that logging and alerting are working
Engineering	Makes sure new features record significant actions in the audit log, do not log sensitive values, and raise errors so they are monitored
Everyone with access to logs	Uses logs only for security, operations, support and compliance purposes, and never extracts personal data from them for other uses

9. Review

- Alerts are investigated promptly, and handled under the Incident Response Plan where they indicate an incident
- Administrator activity in the audit log is reviewed periodically

In addition:

- Administrator activity, including impersonation of customers' users, is reviewed at least quarterly
- Alarm thresholds and alert recipients are reviewed at least annually, and after any incident where monitoring did not detect a problem promptly
- This policy is reviewed at least annually

10. Related Documents

- Information Security Policy
- Incident Response Plan
- Access Control Policy
- Data Classification Policy
- Data Retention & Deletion Policy

- Vulnerability Management Policy
- Business Continuity & Disaster Recovery Policy

11. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and after significant changes to the platform or its monitoring
Effective	October 2026

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.