Information Security Policy

1. Purpose

This Information Security Policy establishes the governance, principles, and minimum control requirements for protecting Subcontext Ltd ("Subcontext") information assets.

The objective of this policy is to ensure the confidentiality, integrity, and availability (CIA) of:

- Customer data
- Platform infrastructure
- Internal systems and communications
- Intellectual property

This policy is designed to align with the Trust Services Criteria defined by SOC 2 and to support ongoing risk management and regulatory compliance obligations.

Subcontext's customers are UK insurers, brokers and other regulated firms, many of them supervised by the FCA and some by the PRA. They trust us with conversations, applications, policies, claims and payment arrangements belonging to their own customers. This policy is the top-level document of our security programme: it sets the rules, and the more detailed policies listed in section 25 explain how each rule is applied.

2. Scope

This policy applies to:

- All employees, contractors, and temporary staff
- All third parties with access to Subcontext systems or data
- All information systems, applications, and infrastructure owned or operated by Subcontext

It covers all data processed or stored by Subcontext, including customer data, operational data, security and audit logs, and backup data.

In practice this includes the web application, background processing, REST API, MCP server, embeddable widgets, the iOS, Android and Mac apps, the AWS infrastructure they run on, source code and build pipelines, company devices, and the business systems the team uses day to day. It covers data whichever channel it arrives through: web chat, SMS, WhatsApp, email, voice or integrations with customers' systems.

3. Definitions

Term	Meaning
Information asset	Any data, system, device, application or account that has value to Subcontext or its customers

Term	Meaning
Customer data	Data that customers or their customers provide to, or generate in, the platform. Subcontext processes it as a processor on the customer's behalf.
Personnel	Directors, employees, contractors and temporary staff
Confidentiality	Information is available only to those authorised to see it
Integrity	Information is accurate and complete and is changed only in authorised ways
Availability	Information and systems are accessible when authorised users need them
Security Officer	The member of the founding team designated to own the security programme

4. Principles

Subcontext's approach to security rests on these principles:

- **Least privilege.** People and systems get only the access they need, for only as long as they need it.
- **Defence in depth.** No single control is relied on alone: network, application, data and people controls overlap.
- **Secure by default.** Safe settings, such as two-factor authentication for new organisations, are the default, not an option.
- **Separation of tenants.** One customer organisation's data must never be visible to another.
- **Accountability.** Significant actions are attributable to a person and recorded.
- **Proportionality.** Controls are matched to the sensitivity of the data and the risk involved.

5. Roles and Responsibilities

Role	Responsibility
Directors	Approve this policy, set risk appetite, provide the resources the programme needs, and accept risks above the Security Officer's authority
Security Officer	Runs the security programme as set out in section 6.1
Engineers	Build and operate systems in line with the Secure Development Policy and Change Management Policy, and protect the production access they hold
All personnel	Follow this policy, protect the information they handle, complete training, and report suspected incidents or weaknesses promptly
Third parties	Meet the security requirements in their contracts and in the Supplier Risk Management Policy

6. Information Security Governance

6.1 Oversight

Subcontext maintains an information security programme overseen by a designated Security Officer (a member of the founding team), who is responsible for:

- Maintaining the security programme and policies
- Ensuring risks are identified and managed
- Coordinating incident response activities
- Reporting on security posture to leadership

The Security Officer reports to the directors at least quarterly on the risk register, incidents, vulnerability remediation, and progress on improvement actions.

6.2 Policy Management

- Security policies and procedures are documented, approved, and communicated
- Policies are reviewed at least annually or upon significant changes
- Version control and change history are maintained

Policies are approved by the directors. Personnel confirm that they have read and understood the policies relevant to their role when they join and whenever a policy changes materially.

6.3 Security Awareness

- All personnel receive security awareness training at onboarding
- Refresher training is conducted at least annually
- Training includes phishing awareness, credential security, and data handling

Engineers also receive secure development training, as described in the Secure Development Policy. Completion of training is recorded.

7. Risk Management

Subcontext operates a formal risk management process designed to identify, assess, and mitigate information security risks.

7.1 Risk Identification

Risks are identified through periodic reviews, system changes, and incident learnings. Threats include technical, operational, and third-party risks.

Other sources include penetration test results, vulnerability findings, supplier assessments, data protection impact assessments, customer due diligence questions and changes in law or regulation.

7.2 Risk Assessment

Risks are evaluated based on likelihood and potential impact. Impact considers customer data, service availability, and reputational harm.

Each risk is scored for likelihood and impact on a scale of 1 (low) to 3 (high), and the two scores are multiplied:

Score	Rating	Expected treatment
6 to 9	High	Treated as a priority, with a mitigation plan agreed by the directors
3 to 4	Medium	Mitigated within a planned timescale, or formally accepted by a director

Score	Rating	Expected treatment
1 to 2	Low	May be accepted by the Security Officer and monitored

For example, a risk that a sub-processor suffers a breach exposing customer conversations might score likelihood 1 and impact 3, giving 3 (Medium). It would be mitigated through supplier due diligence, contractual terms and limiting the data shared with that supplier.

7.3 Risk Treatment

Risks are addressed through mitigation, acceptance, or transfer. Mitigation measures are tracked to completion.

Risk acceptance is always recorded with the reason, the person accepting it and a date for review. Risks rated High may be accepted only by the directors.

7.4 Risk Register

A risk register is maintained and reviewed periodically. Each risk has an assigned owner and status.

The register is reviewed in full at least annually, and individual entries are updated whenever an incident, change or finding affects them.

8. Asset Management

- Subcontext maintains an inventory of key information assets, including production systems, data stores, and code repositories
- Assets are assigned owners responsible for their security
- Acceptable use requirements apply to all systems and devices
- Assets are classified according to sensitivity and criticality

Production infrastructure is defined as code, so the code itself serves as an accurate, version-controlled record of the cloud assets in use. The inventory is reviewed at least annually and when systems are added or retired. Assets that are retired have their data deleted or securely disposed of.

9. Acceptable Use

Personnel must:

- Use Subcontext systems and data only for legitimate business purposes
- Never access customer data except where needed to provide the service, support a customer at their request, or investigate an incident
- Keep their credentials to themselves and never share accounts, passwords or two-factor devices
- Never copy customer data to personal devices, personal accounts or unapproved services
- Never paste customer data or secrets into tools or services that have not been approved for that purpose
- Lock their screen when away from their device and take care when working in public places
- Report lost or stolen devices, and suspected incidents, immediately

10. Data Protection

10.1 Data Classification

Information is classified in accordance with the Data Classification Policy. Security controls are applied proportionately based on classification level.

10.2 Encryption

- Data in transit is encrypted using TLS 1.2 or higher
- Sensitive data at rest (including integration credentials, authentication secrets, and API keys) is encrypted using AES-256
- Database connections use encrypted channels
- Encryption keys are securely stored, access-controlled, and rotated where appropriate
- Backups are encrypted at rest

Details are set out in the Encryption & Key Management Policy.

10.3 Data Handling and Segregation

- Customer data is logically segregated between tenants at the organisation level
- Access to data is restricted based on least privilege and business need
- Production data is not used in non-production environments unless anonymised

Card details are never stored by Subcontext: card payments are handled by Stripe.

10.4 Data Retention and Deletion

Data is retained and deleted in accordance with the Data Retention & Deletion Policy. Customer data deletion requests are handled in accordance with contractual obligations and the Data Processing Agreement.

Many categories of data are deleted automatically when their retention period ends. The return and deletion of data when a customer leaves is covered by the Exit Plan & Data Return Policy.

10.5 Privacy

Subcontext processes personal data in accordance with applicable data protection laws, including the UK GDPR and the Data Protection Act 2018. Principles applied include data minimisation, purpose limitation, and protection of data subject rights.

Subcontext is a processor for customer data and a controller for data about its own users and contacts. Requests from individuals are handled under the Data Subject Rights Procedure, and new high-risk processing is assessed through a data protection impact assessment.

10.6 AI Processing

AI features are governed by the AI Ethics & Responsible Use Policy. Content from outside the platform that AI models read is treated as untrusted and separated from instructions, and baseline guardrails against prompt injection, jailbreak attempts and system prompt extraction are applied to every inbound message.

11. Access Control

- Access to systems and data follows the principle of least privilege
- Role-based access control is used where practical
- Multi-factor authentication (MFA) is enforced for administrative and sensitive access
- User access provisioning and deprovisioning follow documented procedures
- Access rights are reviewed periodically and upon role changes
- Shared accounts are prohibited unless explicitly approved and controlled
- Detailed access control requirements are set out in the Access Control Policy

Within the product, users hold one of three roles (owner, manager or user). Two-factor authentication is enforced by default for new organisations and for Subcontext's own administrative organisation. When a Subcontext administrator acts within a customer's account to provide support, the start and end of that session, and every action taken during it, are recorded against the administrator in the audit log.

12. Endpoint and Device Security

- All company-managed devices must use full disk encryption
- Devices require strong authentication (password or equivalent)
- Devices automatically lock after a period of inactivity
- Systems are kept up to date with security patches
- Use of untrusted or unmanaged devices to access sensitive systems is restricted
- Endpoint protections (operating system security controls) must be enabled

Lost or stolen devices must be reported immediately, so that sessions can be ended and credentials rotated. Devices are wiped before they are reassigned or disposed of.

13. Infrastructure Security

- The platform is hosted on Amazon Web Services (AWS) in the EU (Ireland) region
- Cloud provider security responsibilities are defined under the AWS shared responsibility model
- AWS provides physical security, network security, and infrastructure certifications (ISO 27001, SOC 2)
- Production environments are isolated from non-production environments
- Network access is restricted using security groups and access control lists
- Administrative access is tightly controlled and logged
- Infrastructure is managed as code with version-controlled configurations
- Application servers and databases run in private network subnets, with no direct internet access
- Network traffic is logged (VPC Flow Logs)
- A web application firewall (AWS WAF) applies managed protections and per-IP rate limits in front of the platform
- Production container images are immutable once published, scanned on push, and run as a non-root user

Application servers run across two availability zones and are replaced automatically if they fail health checks. Infrastructure alarms on the database, cache, load balancer and application servers alert the team by email. The database is protected against accidental deletion.

14. Application Security and Secure Development

Subcontext follows secure software development practices, including:

- Security considerations are incorporated into system design
- Code changes are reviewed prior to deployment
- Input validation, output encoding, and parameterised queries are enforced
- Dependencies are monitored for known vulnerabilities using automated tools (Bundler Audit, Brakeman)
- The platform includes CSRF protection, secure session management, and account lockout mechanisms
- A strict Content Security Policy, HTTPS-only access with HSTS, and request rate limiting protect the web application
- Webhooks from external services (payments, messaging, email) are signature-verified and rejected if the signature fails
- API access uses OAuth 2.0 with PKCE; access tokens expire after 2 hours and secrets are stored hashed
- Sensitive functionality (authentication, permissions, data access) receives additional review

Passwords are hashed with bcrypt. Accounts are locked for 10 minutes after 3 failed sign-in attempts, password reset links expire after 6 hours, and sessions expire after 30 days of inactivity. Changing a password or turning off two-factor authentication ends the user's other sessions. The full standards are set out in the Secure Development Policy.

15. Change Management

- Changes to production systems are documented, reviewed, and approved prior to deployment
- Changes are tracked through version control systems
- Emergency changes are logged and reviewed retrospectively
- Rollback procedures are defined for critical systems
- Detailed change management procedures are set out in the Change Management Policy

Every production release requires approval in the deployment pipeline, and a previous release can be redeployed if a problem is found.

16. Secrets and Key Management

- Secrets (API keys, credentials, tokens) are stored in secure managed services
- Secrets must not be stored in source code, configuration files, or logs
- Access to secrets is restricted and auditable
- Secrets are rotated periodically and upon suspected compromise

Production database, cache and application master keys are held in AWS Secrets Manager. Full requirements are in the Encryption & Key Management Policy.

17. Vulnerability Management

- Systems and dependencies are regularly scanned for vulnerabilities
- Vulnerabilities are prioritised based on severity and risk
- Remediation timelines are defined based on criticality
- Security patches are applied in a timely manner
- Detailed vulnerability management procedures are set out in the Vulnerability Management Policy

External researchers can report vulnerabilities under the Vulnerability Disclosure Policy.

18. Monitoring and Logging

- All significant user and system actions are logged in an immutable audit trail
- Logs include timestamps, user identity, IP address, action type, and target
- API requests and LLM API calls are logged for security and cost monitoring
- Security-relevant events (failed logins, account lockouts, privilege changes) are monitored
- Logs are protected from unauthorised access or modification: audit log entries cannot be altered once written
- Compliance decisions are recorded in a tamper-evident, hash-chained trail that is sealed every minute
- Logs are retained for a defined period in accordance with the Data Retention & Deletion Policy
- Alerts are configured for suspicious or anomalous activity

Sensitive values are filtered from application logs. Application errors are monitored continuously, with email alerts when a new error appears, an old one returns or the rate of an error rises. Further detail is in the Logging & Monitoring Policy.

19. Incident Response

Subcontext maintains an Incident Response Plan covering detection, classification, containment, remediation, communication, and post-incident review. All personnel are required to report suspected incidents promptly.

Customers are notified of personal data breaches affecting their data without undue delay, in accordance with the Data Processing Agreement.

20. Business Continuity and Disaster Recovery

Business continuity and disaster recovery are managed in accordance with the Business Continuity & Disaster Recovery Policy, including regular backups, defined recovery objectives (RTO/RPO), and periodic testing of restoration procedures.

How these arrangements support customers' own resilience obligations is summarised in the Operational Resilience Statement.

21. Third-Party Risk Management

- Vendors and sub-processors are evaluated for security prior to engagement
- Security and data protection requirements are contractually enforced
- The current sub-processor list is maintained and available to customers
- Third-party risks are periodically reassessed

Details are set out in the Supplier Risk Management Policy and the Sub-Processor List. Transfers of personal data outside the UK are assessed in the Transfer Risk Assessment.

22. Personnel Security

- Personnel are required to sign confidentiality agreements
- Background checks are performed where appropriate
- Security responsibilities are communicated during onboarding
- Access is revoked promptly upon termination or role change
- Policy violations may result in disciplinary action

Further detail is set out in the Staff Security Policy. Concerns about wrongdoing can be raised under the Whistleblowing Policy.

23. Compliance and Audit

- Subcontext designs its controls to align with the SOC 2 Trust Services Criteria. It does not yet hold an independent SOC 2 report
- Evidence is retained to support audits and customer due diligence
- Control effectiveness is periodically reviewed
- Identified control gaps are tracked and remediated

The Security Officer checks compliance with this policy through periodic control reviews, sampling of records (such as access reviews, change approvals and training completion), and the findings of incidents and penetration tests. Results are reported to the directors.

23.1 Exceptions

Where a requirement of this policy cannot be met, an exception must be requested from the Security Officer before the departure takes place. The request states the requirement affected, the reason, the risk, any compensating controls and an end date. Exceptions are approved by the Security Officer, or by a director where the risk is rated High, and are recorded in the risk register and reviewed before they expire.

23.2 Breaches of Policy

Breaches of this policy may result in disciplinary action, up to and including dismissal or termination of a contract, and may be reported to the authorities where the law requires.

24. Policy Review

This policy is reviewed at least annually and updated to reflect changes in business operations, technology, regulatory requirements, and emerging threats.

25. Related Documents

- Access Control Policy
- Data Classification Policy
- Encryption & Key Management Policy
- Secure Development Policy
- Change Management Policy
- Vulnerability Management Policy
- Vulnerability Disclosure Policy
- Logging & Monitoring Policy
- Incident Response Plan
- Business Continuity & Disaster Recovery Policy
- Operational Resilience Statement
- Supplier Risk Management Policy
- Sub-Processor List
- Transfer Risk Assessment
- Data Retention & Deletion Policy
- Data Subject Rights Procedure
- Data Protection Impact Assessment
- Exit Plan & Data Return Policy
- AI Ethics & Responsible Use Policy
- Staff Security Policy
- Whistleblowing Policy

26. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and upon significant changes
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.