Access Control Policy

1. Purpose

This policy establishes access control requirements for Subcontext systems and data. It sets out who may access what, how that access is granted, authenticated, reviewed and removed, and how access is recorded so that it can be checked afterwards.

Our customers are UK insurers, brokers and other regulated firms. Many of them must show their regulators that a service provider handling their data controls access to it as carefully as they would themselves (for example under FCA SYSC 8 and PRA Supervisory Statement SS2/21). This policy is written to give them that assurance.

2. Scope

This policy applies to:

- **People:** the founding team, any employees, contractors and temporary staff, and customer users of the platform
- **Systems:** the Subcontext web application and dashboard, the REST API and MCP server, the iOS, Android and Mac apps, the AWS production environment (application servers, database, cache, file storage and container registry), source code repositories, the release pipeline, and the third-party services we use to run the platform
- **Data:** customer data held as processor, and Subcontext's own data held as controller, in every environment where it is stored or processed

3. Definitions

Term	Meaning
Customer user	A person given an account in a customer's organisation on the platform
Platform administrator	A Subcontext team member who is a member of Subcontext's own admin organisation on the platform
Production access	Any access to the live AWS environment, its database, cache, file storage, secrets or logs
Privileged access	Production access, platform administrator access, and the ability to change code or infrastructure that reaches production
Impersonation	A platform administrator viewing the platform as a customer user, for support purposes
Two-factor authentication (2FA)	A second check in addition to a password; on the platform this is a time-based one-time code (TOTP), a backup code or an in-app sign-in approval. "MFA" in this policy means the same thing

4. Principles

- **Least privilege:** users are granted the minimum access necessary to perform their role
- **Need-to-know:** access to data is restricted to those who require it for their work
- **Separation of duties:** critical operations require independent verification where practicable
- **Default deny:** access that has not been granted is refused
- **Accountability:** every account belongs to one named person, and privileged actions are attributable to that person
- **Customer control:** customers decide who in their organisation has access to their data, and what role they hold

5. Roles and Responsibilities

Role	Responsibility
Directors	Approve this policy and accept any exceptions to it
Security Officer (a member of the founding team)	Owns this policy, runs the access reviews, keeps the record of privileged access, and approves privileged access requests
Platform administrators	Use administrative access only for support, operations and security purposes, and only for as long as needed
Customer organisation owners	Manage their own users, roles and two-factor settings, and remove users who leave
Everyone with an account	Protects their credentials, uses only their own account, and reports suspected compromise straight away

6. Authentication

6.1 Requirements

- All user accounts require strong passwords (minimum 12 characters)
- Multi-factor authentication (MFA) is required for all administrative and production access
- Session tokens are time-limited with automatic expiry
- Account lockout is enforced after repeated failed authentication attempts

6.2 How the platform enforces this

Control	How it works
Password storage	Passwords are stored only as bcrypt hashes (cost factor 12), never in a readable form
Account lockout	An account is locked for 10 minutes after 3 failed sign-in attempts
Sign-in rate limits	Sign-in attempts are rate-limited per IP address and per email address
Password reset	Reset links expire after 6 hours

Control	How it works
Two-factor authentication	TOTP codes, backup codes and in-app sign-in approval are supported. 2FA is enforced by default for new organisations, and always enforced for Subcontext's admin organisation
Session expiry	Signed-in sessions expire after 30 days of inactivity
Session revocation	Changing a password, or turning off 2FA, ends the user's other sessions
API and app access	OAuth 2.0 with PKCE, scoped access, access tokens that expire after 2 hours, and tokens and client secrets stored only in hashed form

7. Role-Based Access

7.1 Platform (Customer-Facing)

Role	Permissions
Owner	Full organisation management, billing, user management, all features
Manager	Agent configuration, conversation management, data management, user management
User	Agent interaction, conversation viewing, limited configuration

Each customer's data is separated by organisation. A customer user can see only the organisations they belong to. Some sensitive actions are limited to owners and managers, for example erasing a lead's personal data, which also requires a recorded reason.

7.2 Internal (Subcontext Staff)

Role	Permissions
Administrator	Platform administration, customer support, system configuration
Developer	Code deployment, infrastructure management, debugging

Platform administrators are the members of Subcontext's admin organisation. A person holds only the internal roles their work needs.

7.3 Access to customer data by Subcontext staff

Subcontext staff access customer data only to provide the service, to give support the customer has asked for, to investigate a security or operational issue, or where the law requires it. When a platform administrator impersonates a customer user:

- The start and end of the impersonation are recorded in the audit log
- Every action taken during it records the administrator who took it, as well as the user being impersonated
- Impersonation is used for the specific support task and ended when the task is done

8. Access Requests and Approval

1. Access is requested for a named person, stating the system, the level of access and the reason.

2. The Security Officer checks that the access matches the person's role and approves or refuses it. Privileged access granted to the Security Officer is approved by another director.
3. Access is set up under the person's own account. Shared accounts are not used where an individual account is available.
4. The grant is recorded, including who approved it and when.

Customer users are added by their own organisation's owners or managers. Subcontext does not add users to a customer organisation unless the customer asks.

9. Onboarding and Offboarding

- Access is provisioned upon joining and scoped to the employee's role
- Access is reviewed when roles change
- All access is revoked within 24 hours of departure
- Shared credentials are rotated upon any team change

When someone leaves, the leaver's platform account, AWS access, source code access, pipeline access and access to supplier consoles are removed, and the removal is recorded. Deleting a user account on the platform removes their personal details and revokes their sessions, tokens and registered devices.

10. Credential Management

- Passwords must not be reused across services
- API keys and secrets are stored in encrypted configuration, never in code repositories
- Integration credentials provided by customers are encrypted at rest (AES-256)
- Credentials are rotated periodically and upon any suspected compromise

In practice, production secrets (database, cache and application master key) are held in AWS Secrets Manager and Rails encrypted credentials. Customer integration credentials, webhook secrets and similar values are encrypted in the application with AES-256-GCM before they are stored. Sensitive values are filtered out of application logs.

11. Remote and Production Access

- All remote access to production systems requires MFA
- Administrative access is logged in the audit trail
- Production database access is restricted and logged

The production environment runs in private network subnets that are not reachable directly from the internet. Changes to infrastructure are made through version-controlled infrastructure code, and releases pass a manual approval stage before they reach production. Direct changes to production data are made only where a support or operational need cannot be met through the application, and are limited to what that need requires.

12. Logging of Access

The platform's audit log records who did what, when, from which IP address and user agent, and on which request, including the administrator acting on a customer's behalf. Audit log entries cannot be changed once written, and are kept for 2 years.

13. Review

Access permissions are reviewed at least quarterly by the founding team.

Each review covers:

- Every holder of privileged access, checked against their current role
- Membership of Subcontext's admin organisation
- Accounts on supplier consoles and source code repositories
- Any access granted as an exception (section 14)

Access that is no longer needed is removed, and the outcome of the review is recorded. Customers are responsible for reviewing their own users, and we recommend they do so at least quarterly too.

14. Exceptions

An exception to this policy is allowed only when a clear business need cannot be met within it. Each exception is requested in writing, assessed for risk by the Security Officer, approved by a director, time-limited, and recorded. Exceptions are reviewed at every quarterly access review and removed when they expire.

15. Compliance

Compliance with this policy is checked through the quarterly access reviews, the audit log, and the annual review of this policy. A breach of this policy is handled as a security incident under the Incident Response Plan, and may lead to disciplinary action under the Staff Security Policy.

16. Related Documents

- Information Security Policy
- Staff Security Policy
- Encryption & Key Management Policy
- Logging & Monitoring Policy
- Change Management Policy
- Incident Response Plan
- Data Classification Policy

17. Document Control

Item	Detail
Owner	Security Officer

Item	Detail
Approved by	The directors of Subcontext Ltd
Review	At least annually, and after any significant change to the platform or team
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.