Staff Security Policy

1. Purpose

This policy sets out the security responsibilities of everyone who works for or with Subcontext, from joining to leaving.

Our customers are regulated firms who trust us with their customers' personal and financial data. The people who build and run the platform are part of how that data is protected, so this policy describes what we check before someone joins, what we expect while they work with us, and what happens when they change role or leave.

2. Scope

This policy applies to directors, employees, contractors and anyone else who is given access to Subcontext systems or data, wherever they work. In this policy, "staff" means all of these people.

It covers company systems (including the Subcontext platform, its administration area, our cloud infrastructure, source code and business tools) and any device used for Subcontext work.

3. Roles and Responsibilities

Who	Responsibilities
Directors	Own this policy, make sure checks, training and access changes happen, and decide on exceptions
Security Officer	A member of the founding team who runs the security programme, delivers or arranges training, keeps joiner and leaver records, and checks compliance
Everyone	Follows this policy, completes training, and reports incidents and suspicious activity straight away

4. Before Joining

- Right to work is verified
- Background checks are carried out in proportion to the role and the data it can access
- Everyone signs a confidentiality agreement before receiving access

Background checks for roles with access to production systems or customer data will typically include identity, employment history and references. Checks are carried out lawfully, with the person's knowledge, and the results are kept confidential.

5. Onboarding

- Access is granted only to what the role needs, in line with the Access Control Policy
- Everyone completes security awareness training, covering phishing, passwords, data handling and how to report an incident

- Everyone confirms they have read this policy and the Information Security Policy

Onboarding follows these steps:

1. A director confirms the role and the access it needs
2. Accounts are created with two-factor authentication enabled from the start
3. Security awareness training is completed, normally within the first week and before access to customer data
4. The person confirms in writing that they have read this policy and the Information Security Policy
5. The Security Officer records what access was granted and when

Security awareness training is refreshed at least annually, and whenever a significant new risk or a lesson from an incident makes it necessary.

6. Using Company Systems

- Company systems and data are used only for Subcontext's business
- Two-factor authentication is used on every account that supports it, including access to the Subcontext platform's administration area
- Passwords are unique and stored in a password manager
- Customer data is never copied to personal accounts, personal devices or unapproved services
- Suspicious emails, messages and requests are reported, not acted on

In addition:

- Customer data is only accessed when there is a business need, such as resolving a support request the customer has raised. When an administrator acts within a customer's account, the platform records the start and end of that session and every action taken
- Secrets, keys and credentials are never shared in chat, email or source code. They are held in managed secret stores, in line with the Encryption & Key Management Policy
- Customer data is handled according to its classification under the Data Classification Policy
- New tools or services that would hold company or customer data are approved by a director before use

Worked example

A message that appears to come from a director asks for an urgent change to a customer's bank details or for a set of login codes. The recipient does not act on it. They check with the director through a separate, known channel and report the message to the Security Officer, who decides whether it should be handled under the Incident Response Plan.

7. Devices and Remote Working

- Devices used for work have full disk encryption, a screen lock and up-to-date software
- Devices lock automatically when not in use
- Work is done on trusted networks, or over encrypted connections
- Screens are kept private in public places
- Lost or stolen devices are reported immediately so access can be revoked

Security updates are applied promptly, and devices that can no longer receive updates are not used for Subcontext work. Work devices are not shared with family members or others.

8. Reporting Incidents

Anyone who suspects a security incident, a lost device, a mistaken disclosure of data or a breach of this policy reports it straight away to the Security Officer or a director. Reports are handled under the Incident Response Plan. Nobody will be criticised for reporting a genuine concern promptly, including when they made the mistake themselves.

9. Leaving or Changing Role

- Access is reviewed whenever a role changes
- All access is revoked within 24 hours of leaving
- Company devices and data are returned or securely wiped
- Shared secrets the person could access are rotated

The leaver process follows these steps:

1. A director tells the Security Officer the leaving date
2. On or before that date, and no later than 24 hours after it, the person's access to every system is removed, including platform accounts, sessions, tokens and devices
3. Company devices and data are returned or securely wiped
4. Shared secrets the person could access are rotated
5. The person is reminded that their confidentiality obligations continue after they leave
6. The Security Officer records that each step is complete

Where someone leaves in difficult circumstances, access is removed immediately.

10. Exceptions

Any exception to this policy must be approved in advance by a director, recorded with its reason and any compensating controls, and given an end date. Exceptions are reviewed when they expire and at the annual review of this policy.

11. Checking Compliance

- Joiner and leaver records are checked to confirm access was granted and removed on time
- Access is reviewed at least quarterly under the Access Control Policy
- Training completion is tracked
- Platform administration activity is recorded in the audit log and can be reviewed

12. Breaches of This Policy

Breaches of this policy are taken seriously and may lead to disciplinary action. For contractors, a breach may lead to termination of the contract. Where a breach puts customer data at risk, it is also handled under the Incident Response Plan.

13. Related Documents

- Information Security Policy
- Access Control Policy
- Data Classification Policy
- Encryption & Key Management Policy
- Incident Response Plan
- Whistleblowing Policy

14. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors
Review	At least annually, and after any significant incident or change to how we work
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.