



P O L I C Y 1 3 O F 1 6

Information Security Policy

Real partnership. Real expertise.

Document reference	SOMA-POL-13
Version	2.0
Issue date	March 2026
Next review	March 2027
Policy owner	Adam O'Neill, Director
Approved by	Stevie MacGregor
Classification	Public — available on request

SOMA Project Controls Ltdwww.somaprojectcontrols.com

1. Purpose

This policy sets out how SOMA Project Controls Ltd protects the information entrusted to us — by clients, by our people, and by our business — against unauthorised access, loss or misuse.

2. Scope

Applies to all information processed by SOMA in any form, all systems on which it is stored or transmitted, and all personnel with access to it.

3. Guiding Principles

- Confidentiality — information is accessed only by those who need it.
- Integrity — information is accurate, complete and trustworthy.
- Availability — information is available to authorised users when needed.
- Proportionality — controls are matched to the sensitivity of the information and the nature of the risk.

4. Information Classification

Information is handled according to its classification:

- Public — may be shared without restriction (e.g. marketing material, published policies).
- Internal — for use within SOMA and named counterparties (e.g. internal process documents).
- Confidential — restricted to specific individuals (e.g. client project data, personal data).
- Restricted — handled under named-user controls (e.g. client commercially sensitive material under NDA, or security-sensitive information).

5. Access Control

- Unique user accounts — account sharing is prohibited.
- Multi-factor authentication enforced on all cloud services containing Confidential or Restricted data.
- Least-privilege access; access reviews carried out quarterly.
- Joiner, mover and leaver processes executed within one working day of a change.
- Strong password requirements aligned to NCSC guidance.

6. Device & Network Security

- Full-disk encryption on all laptops and mobile devices.
- Supported, patched operating systems only, with automatic updates enabled.
- Licensed, business-grade endpoint protection on all devices.
- Home and public networks used only through a supported configuration; unsecured public Wi-Fi is avoided for Confidential and Restricted work.
- USB and removable-media use is restricted and, where used, encrypted.

7. Data Handling

- Client data is stored only in approved cloud locations — never on personal email, personal cloud storage or unmanaged devices.
- Sharing is by permissioned link or within approved collaboration environments; broad-link sharing is disabled by default.
- Paper is avoided; where used, it is stored in locked storage and shredded on disposal.
- Confidential and Restricted data are encrypted in transit.

8. Third Parties

Before sharing Confidential or Restricted information with a third party, appropriate contractual protections are put in place (for example a non-disclosure agreement and a data-processing agreement). Third-party security posture is assessed proportionate to the sensitivity of the data and the criticality of the service.

9. Incident Management

Suspected information-security incidents must be reported to the Director without delay — within one hour for any incident affecting Confidential or Restricted data. Incidents are investigated, contained, recovered, and reviewed; lessons are captured and acted on. Where personal data is involved, the Data Breach Response section of the Privacy Policy applies.

10. Alignment to Recognised Standards

This policy is written in alignment with the controls expected under Cyber Essentials, and with ISO/IEC 27001 and NCSC guidance. SOMA will progress toward formal certification where client demand justifies the cost.

11. Review & Governance

This policy is reviewed at least annually, and sooner if legislation, SOMA Project Controls Ltd's operating context or client requirements change materially. The Director is the accountable owner. Minor amendments are logged in the version-control table; material changes trigger a re-issue and fresh sign-off by the policy owner and approver named on the sign-off page.

S I G N E D & A P P R O V E D

Policy Adoption & Approval

This policy is formally adopted by SOMA Project Controls Ltd. It is communicated to all employees, associates and, where relevant, supply-chain partners, and is available on request to clients, prospective clients and other interested parties. The signatures below record its adoption and the date from which it takes effect.

P O L I C Y O W N E R*Adam O'Neill***Adam O'Neill**

Director

SOMA Project Controls Ltd

Date: March 2026**A P P R O V E D B Y***Stevie MacGregor***Stevie MacGregor**

Director

SOMA Project Controls Ltd

Date: March 2026**N e x t s c h e d u l e d r e v i e w****March 2027**