



AI Policy Security Standards

Service Definition Document. Version 1.0

21 January 2026

AI Policy Security Standards

1. Introduction

This Service Definition Document describes the AI Policy & Security Standards service offered by Cambridge Cyber Advisers (CCA) under the G-Cloud 15 framework. The service provides organisations with a structured approach to developing AI governance, security controls, and responsible AI policies aligned to regulatory, ethical, and operational requirements.

As AI adoption accelerates, organisations must ensure that AI systems are secure, transparent, compliant, and ethically deployed. CCA's service helps organisations establish robust AI governance frameworks and security standards aligned to NCSC, ISO 27001, ISO 42001, and emerging AI regulations.

2. Service Overview

Activities include:

- Assessment of existing governance and security controls
- AI risk and compliance assessment
- Development of AI governance frameworks
- Creation of AI security standards and control baselines
- Policy development (acceptable use, model governance, data governance)
- Alignment to regulatory requirements (e.g., EU AI Act, UK guidance)
- Responsible AI and ethical considerations
- Executive and technical debrief sessions

Service Features

- AI governance framework development
- AI security standards aligned to industry best practice
- Policy creation and documentation
- Risk and compliance assessment
- Responsible AI and ethical guidance
- Executive reporting and prioritised recommendations

Service Benefits

- Ensures safe, secure, and compliant AI adoption
- Reduces regulatory and operational risk
- Strengthens governance and accountability
- Supports responsible and ethical AI deployment

3. Service Scope

Includes governance, policy development, security standards, and compliance alignment.

4. Delivery Methodology

- Scoping and Planning
- Documentation Review and Stakeholder Interviews
- Policy and Standards Development
- Analysis and Reporting
- Executive and Technical Debrief

5. Deliverables

- AI Governance Framework
- AI Security Standards
- Policy Suite (as required)
- Risk Register
- Remediation Roadmap

6. Service Levels

- Engagement begins within 10 working days
- Draft policies within 10 working days
- Final outputs within 15 working days

7. Governance and Assurance

Aligned to ISO 42001, ISO 27001, NCSC, and responsible AI frameworks.

Backup and Restore

Not applicable — this service does not handle customer production data or operate within customer systems in a way that requires backup/restore functionality.

Reporting & Analytics

Outputs include:

- AI Governance Framework
- AI Security Standards
- Policy Suite (as required)
- Risk Register
- Remediation Roadmap

Incident Management

- Not Applicable. This is a purely advisory service.

Disaster Recovery

Not applicable — service is not hosted and does not rely on persistent operational infrastructure.

Availability

Service availability applies only to consultant scheduling. CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time with out-of-hours engagements available on request.

8. Security and Data Protection

- Confidential handling of customer data
- UK-based assessment team
- GDPR-aligned practices

Staff Security Clearance

SC cleared staff available on request. Baseline Personnel Security Standard (BPSS) checks conducted for all consultants.

9. Customer Responsibilities

Customers are responsible for providing accurate scoping information, nominating escalation contacts, supporting internal approvals, and implementing remediation actions.

Technical Requirements

- Defined scoping information (target systems, domains, cloud environments)
- Access to key stakeholders (security, IT, Legal, Risk/Compliance)

No agent installation is required unless explicitly scoped.

Supported Browsers/Devices

Not applicable — this is a consultancy service, not a hosted software product.

Access Restrictions

Customer must designate authorised individuals for:

- Scope approval
- Rules of Engagement
- Emergency halt
- Receipt of confidential outputs

10. Service Constraints

Limited to agreed scope.

11. Pricing

Pricing is engagement-based and determined by scope, duration, and complexity. Pricing is based on:

- Scope
- Complexity of environments
- Duration of engagement
- AI Tools used

Typical engagements range from 2–8 weeks.

Day-rate pricing is available on the pricing document and compliant with G-Cloud pricing rules.

Ordering and Invoicing Process

Ordering from clients is generally done via the presentation of a Purchase Order following confirmation of the purchase of a service. CCA will invoice at the end of every calendar month, giving a precise breakdown of the services purchased, including VAT/other expenses. CCA can provide consolidated invoices if required. Invoices can be issued electronically or via post.

12. Exit and Offboarding

At engagement end, all findings are delivered, knowledge transfer sessions completed, and customer data securely destroyed. Certificates of destruction can be provided.

Onboarding:

- Requirements workshop
- Definition of scope, assets, and Rules of Engagement
- Identification of critical assets, defensive technologies, and response processes
- Validation of communication protocols and escalation points

Offboarding:

- Full walkthrough of all findings
- Delivery of policies, evidence and artefacts
- Secure data destruction within 30 days post-engagement (certificate provided)

Training Provided

- Awareness session explaining policies and their application within the environment

13. Termination

- Standard G-Cloud termination terms apply
- Customer may terminate with notice; work completed to date will be invoiced
- Provider may terminate only under defined exceptions (e.g., breach of Rules of Engagement or safety concerns)

14. Contact and Support

A delivery manager is assigned for each engagement. Support is available via email and phone during delivery hours.

Included as standard:

- Email and phone support during the engagement
- Delivery manager assigned
- Access to reporting team for clarifications

Enhanced support packages available for continuous testing programmes.