# CODE OF CONDUCT – ACCREDITED COMPANIES

## 1. Executive Summary & Purpose

This Code of Conduct sets clear principles, standards, and behaviours for companies and individuals operating under The Cyber Scheme's Accreditation Programme. It is designed to protect all parties, strengthen trust across the cyber security ecosystem, and promote positive, measurable engagement. While no single code can anticipate every situation, partners are expected to uphold the spirit as well as the letter of this Code and to exercise sound judgement in complex or novel scenarios.

This Code aligns with The Cyber Scheme's mission to professionalise the cyber workforce, promote quality, transparency, and resilience, and connect industry, government, and academia in a verified talent ecosystem.

## 2. Scope

**In scope:** All The Cyber Scheme Accredited Companies (Global and Specialism-based) and Professionally Registered Individuals providing or receiving services under agreements, contracts or tenders that reference The Cyber Scheme and/or are delivered as The Cyber Scheme-accredited assignments.
**Out of scope:** Companies not enrolled in The Cyber Scheme accreditation programme, and engagements that do not reference The Cyber Scheme or fall outside the company's accredited specialisms.

## 3. Definitions

**Accredited Company (AC):** A company approved by The Cyber Scheme as Global or Specialism-based after verification of independently audited certification. Example Technical Certifications: Cyber Essentials Plus. Example Organisational Security Requirements: ISO27001, IASME Cyber Assurance, *and* the presence of at least One Qualifying Personnel per specialism.
**Specialisms:** Security Testing; Incident Response; Secure Operations; Governance & Risk Management; Secure System Architecture & Design; Cyber Security Audit & Assurance; Cyber Security Management; Operational Technology (OT). More to be added.

All Rights Reserved | The Cyber Scheme 2026 version 2.0 | all enquiries: info@thecyberscheme.org

**Qualifying Personnel:** Individuals holding PCSP or ChCSP (professional titles recognised by The Cyber Scheme and awarded by the UK Cyber Security Council) identified per specialism to underpin competency.
**Certified Individual:** A person holding recognised certification(s) and engaged in The Cyber Scheme-referenced services for or on behalf of an AC.

### 4. Jurisdiction

This Code is governed by the laws of England and Wales; parties submit to the jurisdiction of the courts of England and Wales.

### 5. Governance, Complaints & Independence

The Cyber Scheme maintains an independent complaints handling mechanism. Accredited Companies must cooperate fully with any investigations. The Cyber Scheme verifies capability, controls, and competence as part of accreditation; however, it does not underwrite assignments and will not be liable for services delivered by partners.

### 6. Core Conduct Requirements (All Accredited Companies)

**Promotion of Good Practices**

- Implement and continuously improve quality and security management systems appropriate to their services.
- Maintain adequate professional insurances.
- Operate robust personnel vetting, access control, and data handling aligned to accreditation commitments.
- Provide a clear complaints procedure and resolve complaints effectively.
- Notify The Cyber Scheme promptly of suspected breaches of NDAs or lack of integrity during a Professional Registration assessment.
- Foster a diverse, equitable and inclusive workplace.

**Professional Representation**

- Represent The Cyber Scheme professionally to clients and partners; use branding per guidelines (provided upon request).
- Avoid any action that could bring The Cyber Scheme or the profession into disrepute.

All Rights Reserved | The Cyber Scheme 2026 version 2.0 | all enquiries: info@thecyberscheme.org

**Regulations & Compliance**

- Maintain knowledge of and compliance with relevant laws and regulations.
- When operating abroad, comply with local legislation and ethical guidance.

**Competencies & Professional Development**

- Keep current with threats, vulnerabilities, and countermeasures.
- Encourage internal incident reporting and learning culture.
- Provide ongoing professional development.

**Client Interests**

- Act with objectivity, independence, and professional judgement.
- Safeguard confidentiality and handle client information lawfully.
- Disclose interests in products/services recommended to the client.

**Ethics**

- Companies and Certified Individuals agree to comply with this Code and The Cyber Scheme's Code of Ethics as well as the Code of Ethics of the UK Cyber Security Council and accept accountability for violations.

**Sanctions**

- Breaches may result in suspension or revocation of accreditation, restrictions on exam participation, and legal action.

**7. Additional Requirements (The Cyber Scheme-Accredited Assignments)**

- Ensure all personnel engaged in The Cyber Scheme assignments understand and apply the Company's approved policies, procedures, and methodologies.
- Make clients aware of The Cyber Scheme's independent complaints mechanism.
- Notify The Cyber Scheme within 30 days when a Qualifying Personnel change impacts the company's accredited status.

All Rights Reserved | The Cyber Scheme 2026 version 2.0 | all enquiries: info@thecyberscheme.org

## 8. Requirements for Professionally Registered Individuals

**Certified Individuals operating under a The Cyber Scheme-Accredited Assignment will:**

- Be familiar with and comply with the AC's approved policies, procedures, methodologies and The Cyber Scheme's Code of Ethics (see above).
- Operate strictly within the bounds of their competence and certifications.
- Uphold integrity and confidentiality obligations.

## 10. Acknowledgement

By signing, the Accredited Company and any Certified Individuals engaged acknowledge they have read, understood, and agree to abide by this Code of Conduct and The Cyber Scheme's Code of Ethics as well as the Code of Ethics of the UK Cyber Security Council

**Name:** **Role:** **Company:**

**Signature:** **Date:**

All Rights Reserved | The Cyber Scheme 2026 version 2.0 | all enquiries: info@thecyberscheme.org