CLOUDGAP LTD

Supplier Code of Conduct & Whistleblowing Policy

Document Reference: CG-POL-SCW-001

Version: 1.0

Effective Date: 1 October 2026

Review Date: Annual (October 2027)

Approved By: Board of Directors, Cloudgap Ltd

PART A: SUPPLIER CODE OF CONDUCT

1. Introduction & Scope

Cloudgap Ltd is committed to the highest standards of ethical conduct, cybersecurity, and operational integrity. As a trusted partner to UK Critical National Infrastructure (CNI), central government, and regulated enterprises, we expect our supply chain to reflect these same standards.

This Code of Conduct applies to all third-party suppliers, software vendors, associate consultants, and subcontractors (collectively, "Suppliers") providing goods or services to Cloudgap Ltd.

2. Ethical Business Practices

- **Anti-Bribery and Corruption:** Suppliers must comply fully with the UK Bribery Act 2010. Bribes, kickbacks, or any improper inducements are strictly prohibited.
- **Conflicts of Interest:** Suppliers must disclose any potential or actual conflicts of interest relating to their engagement with Cloudgap Ltd or our end-clients.

3. Human Rights and Labor Standards

- **Modern Slavery:** In alignment with the Modern Slavery Act 2015, Suppliers must not use forced, bonded, or involuntary prison labor. Suppliers must take proactive steps to ensure human trafficking and modern slavery do not exist within their own supply chains.
- **Equality and Diversity:** Suppliers must comply with the Equality Act 2010, ensuring a workplace free from discrimination, harassment, and victimisation based on any protected characteristics.

- **Fair Treatment:** Suppliers must provide fair compensation, adhere to statutory working hour limits, and ensure a safe and healthy working environment for all personnel.

4. Cybersecurity, Data & AI Governance

Given Cloudgap's role in delivering NCSC CAF readiness, AI security, and our GRC 360 Assure platform, Suppliers must adhere to strict digital standards:

- **Information Security:** Suppliers must protect all confidential and sensitive information. Where applicable, Suppliers must maintain at minimum a valid Cyber Essentials certification.
- **Data Protection:** Suppliers must comply with the UK GDPR and Data Protection Act 2018, ensuring no unauthorized transfer of data outside agreed residency boundaries.
- **Personnel Vetting:** Any Supplier personnel accessing Cloudgap or client systems must hold the appropriate security clearance (e.g., BPSS, SC) as mandated by the specific contract.

PART B: WHISTLEBLOWING POLICY

1. Purpose and Commitment

Cloudgap Ltd is committed to conducting business with honesty and integrity. We encourage a culture of openness and accountability. This Whistleblowing Policy provides a secure framework for employees, associate consultants, and Suppliers to report suspected wrongdoing, danger, or illegal activities without fear of retaliation.

2. Scope of Protected Disclosures

This policy covers concerns regarding activities that are in the public interest. "Qualifying disclosures" under the Public Interest Disclosure Act 1998 include, but are not limited to:

- Criminal offenses (e.g., fraud, bribery).
- Breaches of legal or regulatory obligations (e.g., UK GDPR violations).
- Miscarriages of justice.
- Health and safety risks.
- Environmental damage.
- Instances of modern slavery or human trafficking in the supply chain.
- Cover-ups relating to any of the above.

3. Protection and Confidentiality

- **Non-Retaliation:** Cloudgap Ltd strictly prohibits any form of retaliation, discrimination, or detrimental treatment against anyone who raises a genuine concern in good faith, even if the concern is ultimately unsubstantiated.

- **Confidentiality:** All reports will be treated with the utmost confidentiality. While individuals are encouraged to put their names to disclosures to facilitate investigations, concerns can be raised anonymously.

4. How to Raise a Concern

Internal Reporting (For Employees & Associates): In the first instance, concerns should be raised directly with your Line Manager or the Lead Consultant. If the matter is highly sensitive or involves senior management, it should be escalated directly to the Director.

Supplier & Third-Party Reporting: Suppliers, subcontractors, and external partners who witness breaches of the Supplier Code of Conduct or suspect illegal activities associated with Cloudgap operations should report their concerns directly to:

- **Designated Officer:** Pritesh Hathi, Founder & Director
- **Email:** pritesh@cloudgap.ai
- **Mail:** Private & Confidential, Cloudgap Ltd, Avondale House, 262 Uxbridge Road, Hatch End, HA5 4HS

5. Investigation Process

1. **Initial Assessment:** The Director (or an appointed independent investigator) will conduct a preliminary review to determine if a formal investigation is required.
2. **Investigation:** If warranted, a prompt, objective, and confidential investigation will be carried out. The whistleblower may be contacted for further information if they have not reported anonymously.
3. **Outcome and Remediation:** Appropriate corrective actions will be taken based on the investigation's findings. This may include reporting illegal activities to relevant authorities (e.g., the NCSC, ICO, or law enforcement) or terminating non-compliant Supplier contracts.
4. **Feedback:** Where possible and appropriate, the whistleblower will be kept informed of the progress and outcome of the investigation.