Data Protection Policy

1. PURPOSE

This policy applies to **Coresecure Services Ltd** in England. The company is registered with the Information Commissioner's Office (ICO). Our registration details are available on the ICO's website: www.ico.org.uk. The registration number is maintained at the head office and renewed annually.

This policy ensures that Coresecure Services Ltd complies with the UK **Data Protection Act 2018** (incorporating GDPR principles) and ISO 9001 requirements. It outlines how personal data is collected, stored, processed, and protected.

The Data Protection Register provides:

- Details of the purposes for which personal information may be used
- Types of data subjects whose personal information may be held
- Types of personal information that may be processed
- Recipients of personal information
- Any transfers of personal information

Coresecure Services Ltd collects and processes personal data of employees, clients, contractors, and other stakeholders for legitimate business purposes and legal compliance. Personal data will always be processed in accordance with the following principles:

1. Lawful, fair, and transparent processing
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability
8. No transfer outside the UK or EEA without adequate protection

2. RESPONSIBILITY

- **Director** – Ensures the policy is implemented and followed across the company.
- **Data Protection Officer / Management Representative** – Maintains, reviews, and updates this policy regularly.

3. STATUS OF THE POLICY

This document defines Coresecure Services Ltd's policies and procedures for compliance with UK Data Protection legislation. It is available to employees, contractors, and relevant external parties. It does not replace the full text of the law but summarises requirements.

4. DATA CONTROLLER

The **Director of Resources** is the main Data Controller. Local managers and the Data Protection Officer manage day-to-day data protection compliance and support staff in following this policy.

5. CONSENT

Personal data will generally be processed with the consent of the individual. For sensitive data, explicit consent is required. Certain data processing is mandatory for employment, contracting, or service provision. Refusal to consent may limit access to services, roles, or projects.

6. STAFF RESPONSIBILITIES

All employees, including contractors and temporary staff, must comply with this policy. Breaches may result in disciplinary action, including dismissal.

Specific Responsibilities:

- Ensure personal information provided to the company is accurate

- Notify Coresecure Services Ltd of changes to personal data
- Handle third-party data securely and only for legitimate business purposes

Security Measures:

- Data stored in locked cabinets or password-protected electronic systems
- No unauthorised disclosure of personal data
- Off-site processing requires precautions to prevent data breaches

7. CLIENTS AND THIRD-PARTY DATA

- Personal data of clients, suppliers, and other third parties will be processed lawfully and fairly.
- Consent must be obtained where appropriate.
- Individuals may request access, correction, or removal of their data in line with their rights.

8. STUDENT OR TRAINEE DATA (IF APPLICABLE)

Coresecure Services Ltd ensures accurate collection, storage, and use of data for students or trainees in training programs. Data will be used for administrative, auditing, or accreditation purposes, with consent obtained for research or surveys.

9. ACCURACY OF DATA

All personal data must be kept accurate and up to date. Coresecure Services Ltd will take reasonable steps to verify data before processing. Individuals can request corrections or updates, with supporting documentation if needed.

10. DATA SECURITY

- Access to personal data is limited to authorised personnel
- Electronic data is encrypted and backed up
- Paper records are stored securely

- Disposal of personal data follows secure procedures, including shredding or secure deletion

11. DATA RETENTION AND TRANSFER

- Different types of data will be retained according to legal, operational, and contractual requirements
- No personal data will be transferred outside the UK or EEA without explicit consent and appropriate safeguards

12. USE OF PERSONAL DATA IN RESEARCH

Data may be used for research purposes only if it does not identify individuals or cause harm. Statistical and anonymised data may be processed for ISO 9001 reporting and continuous improvement purposes.

13. COMPLIANCE AND MONITORING

Coresecure Services Ltd will:

- Review this policy annually
- Train staff on data protection and ISO 9001 quality management principles
- Investigate any breaches or complaints in line with disciplinary procedures

Signed: 

Date: 04/04/2026