Data Protection Policy

DISTRIBUTION

This Data Protection Policy is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

Introduction

In the course of your work you may come into contact with or use confidential information about employees, clients, customers and suppliers, for example their names and home addresses. The General Data Protection Regulations 2018 contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of this policy is to ensure you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Company's Data Protection Officer (see below). You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

This policy does not form part of an employee's contract of employment but it is a condition of employment that employees abide by this policy and therefore any failure to follow it can result in disciplinary proceedings.

The data protection principles

There are eight data protection principles that are central to the Act. The Company and all employees must comply with these principles at all times in their information handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to

sensitive personal data. The conditions are either that the employee has given his consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

- Race or ethnic origin.
- Political opinions and trade union membership.
- Religious or other beliefs.
- Physical or mental health or condition.
- Sexual life.
- Criminal offences both committed and alleged.

2. Obtained only for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes.

3. Adequate, relevant and not excessive in relation to the purposes for which it is processed. The Company will review employees' personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there is sound business reason requiring information to continue to be held.

4. Accurate and where necessary kept up-to-date. If your personal information changes, for example you change address or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company cannot be responsible for any such errors unless the employee has notified the Company of the relevant change.

5. Not kept for longer than is necessary. The Company will keep personnel files for no longer than seven years after an employee has left the Company's employment. Different categories of data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

6. Processed in accordance with the rights of employees under the Act.

7. Secure Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored as such in locked filing cabinets. Only authorised employees have access to these files. For a list of authorised employees, please contact one of our Area Managers. Files will not be removed from their normal place of storage without good reason. Data stored on diskettes or other removable storage media is kept in locked filing cabinets. Data held on computer is also stored confidentially by means of password protection, encryption or coding and again only the above employees have access to that data. The Company has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection relation to the processing of personal data.

Employees' consent to personal information being held

The Company holds personal data about its employees and, by signing your contract of employment; you have consented to that data about you being processed by the Company. Agreement to the Company processing your personal data is a condition of your employment.

The Company also holds limited sensitive personal data about its employees and, by signing this policy; you give your explicit consent to our holding and processing that data, for example sickness absence records, particular health needs and equal opportunities monitoring data.

Employees' rights to access personal information

Under the Act, employees have the right on request to receive a copy of the personal data that the Company holds about them, including personal data held on personnel files that form part of a relevant filing system, and to demand that any inaccurate data held be

corrected or removed. They also have the right to seek compensation where damage and distress have been caused to them as a result of any breach of the Act by the Company. Employees have the right, on request:

- To be told by the Company whether and for what purpose personal data about them is being processed.
- To be given a description of the personal data concerned and the recipients to whom it is or may be disclosed.
- To have communicated in an intelligible form the personal data concerned, and any information available to the Company as to the source of the data.
- To be informed in certain circumstances of the logic involved in computerised decision-making.

Upon request, the Company will provide you with a statement regarding the personal data held about you. This will state all the types of personal data the Company holds and processes about you and the reasons for which they are processed.

If you wish to access a copy of any personal data being held about you, you must make a written request for this and the Company reserves the right to charge you a fee of £10.00 for the supply of the information requested. If you wish to make a request, please complete a Personal Data Request Form, which can be obtained from the Data Protection Officer. Once completed, it should be returned to the Data Protection Officer. The Company will respond promptly and in any case within 40 calendar days of receiving the request. Note that the Company will always check the identity of the employee making the request before processing it.

If you wish to make a complaint that this policy has not been followed in respect of personal data the Company holds about you, you should raise the matter with the Data Protection Officer / Area Manager. If the matter is not resolved, it should be raised as a formal grievance under the Company's grievance procedure.

Exemptions

There are a number of exemptions from the data protection regime set out in the Act, for example:

- Confidential references that are given, but not those received by the Company from third parties. Only designated line managers can give Company references.
- Confidential references will not be provided unless the Company is sure this is the employee's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Employees' obligations in relation to personal information

You should ensure you comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- If you receive a request for personal information about another employee, you should forward this to the Data Protection Officer, who will be responsible for dealing with such requests.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected.

Compliance with the Act is the responsibility of all employees. Any questions or concerns about the interpretation of this policy should be taken up with the Data Protection Officer.

Health & Safety Policy

DISTRIBUTION

This Health & Safety Policy is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

INTRODUCTION

The Company has drawn up a general safety policy, which must be held in every region and displayed. The statement must be brought to the attention of all Company employees as part of their Induction Training.

The Policy details the arrangements within the Company for ensuring Health, Safety and Welfare and identifies the responsibilities for Health & Safety for all employees at all levels.

The Policy is reviewed at least annually, and any amendments must be brought to the attention of all employees.

POLICY STATEMENT

It is the Company's policy to comply with the Health & Safety measures required by law, including Working Time Regulations and to act positively to ensure that all premises are safe and healthy places in which to work.

The Company also recognises that the Health, Safety and Welfare of all employees, whether on Company premises or carrying out Company business elsewhere, are primarily the responsibility of the management.

The Company recognises its responsibilities for the Health & Safety of others, whilst they are on our premises and our neighbours in the community around us.

All employees are reminded that they have an important duty to conform to Health & Safety Policies and Procedures, also to do everything that is required of them to prevent injury to themselves and others and loss to the Company. To also comply with the various safety requirements of the Working time Regulations.

Within the Company the Regional manager is responsible for implementing this policy. All appropriate resources are made available to ensure that this policy is maintained.

The Company is committed to progressively improving its Health & Safety performance and will monitor the effectiveness of the Policy on a regular basis with a formal review annually.

The policy will be revised as often as may be appropriate following these reviews to ensure continuing improvements in the Health & Safety standards within the Company.

Induction Policy

DISTRIBUTION

This Fatigue Management Policy is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

Introduction

This induction policy outlines the process for welcoming and integrating new employees into Cerberus Security Services Limited. Our objective is to ensure that all new team members receive the necessary information, training, and support to perform their duties effectively and safely, in alignment with our company values and the standards set by the Security Industry Authority (SIA).

Scope

This policy applies to all new employees, including full-time, part-time, and temporary staff within the operational and administrative departments of Cerberus Security Services Limited.

Policy Details

1. **Orientation Session**
    - **Objective:** To introduce new employees to the company's mission, values, and structure.
    - **Content:** Overview of Cerberus Security Services Limited, key contacts, tour of the premises, and introduction to the company culture and expectations.
2. **SIA Licensing and Regulatory Compliance**
    - **Objective:** To ensure new employees understand the importance of SIA licensing and compliance with industry regulations.
    - **Content:** Information on the role of the SIA, the importance of holding a valid SIA license for operational roles, and an overview of key regulations impacting their work.
3. **Health and Safety**
    - **Objective:** To prioritize the health and safety of our employees and clients.
    - **Content:** Health and safety policies, emergency procedures, reporting accidents and incidents, and safe work practices.
4. **Company Policies and Procedures**
    - **Objective:** To familiarize new employees with company-specific policies.
    - **Content:** Detailed review of policies including data protection, equality and diversity, anti-harassment and bullying, and grievance procedures.

5. **Role-Specific Training**
    - **Objective:** To equip new employees with the skills and knowledge required for their specific roles.
    - **Content:** Operational procedures, customer service standards, use of security equipment, and any necessary certifications or training programs.
6. **Mentoring and Support**
    - **Objective:** To provide ongoing support to new employees during their initial period.
    - **Content:** Assignment of a mentor, outline of the support structure, and information on performance reviews and feedback mechanisms.
7. **Feedback and Continuous Improvement**
    - **Objective:** To encourage open communication and continuous improvement.
    - **Content:** Introduction to feedback mechanisms, encouragement to contribute ideas for improvement, and information on how feedback is used to enhance operations.

Implementation

- The induction process begins on the first day of employment and continues over the first month, incorporating both general and role-specific elements.
- HR will coordinate the scheduling of all sessions and ensure completion of all components.
- Line managers are responsible for overseeing the practical integration of new employees into their roles and providing ongoing support and guidance.

Review and Acknowledgment

- Upon completion of the induction program, new employees will be asked to acknowledge in writing that they have received and understood the information provided.
- The HR department will review the induction policy annually or as required by changes in regulations or company operations, ensuring it remains effective and relevant.

This policy is designed to create a supportive, informative, and compliant induction process for all new employees at Cerberus Security Services Limited, laying the foundation for their success and the continued excellence of our services.

Training and Development Policy

DISTRIBUTION

This Training & Development Policy is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

The Private Security Industry Act 2001 has brought into force a licensing system for people working in the private security industry.

This law aims to raise standards in training and professionalism and prevent unsuitable people working within the industry.

To this end the company will ensure that all our Security Guards have the necessary training qualifications before being allowed to work.

The required qualification is the Level 2 National Certificate for Security Guards. This will be delivered by an SIA endorsed Awarding Bodies.

A recognised company will train successful new employees to industry standard. In addition, the company will also liaise with local colleges to help others obtain the qualification needed.

The company will keep a record of the employees' qualification in personnel files as proof of completion of training.

The company will also keep a copy of the employees' SIA badges as proof of acceptance to work in the relevant sectors of the industry.

To develop further an employee can undergo training in other aspects of security – leadership, first aid, etc - the company encourages personal development and will give help and advice when necessary.

TRAINING AND DEVELOPMENT POLICY

1. Policy Statement

Cerberus Security Services Limited is committed to providing appropriate training and development opportunities to ensure that employees have the skills, knowledge, and competence required to perform their roles effectively and safely. We recognise that training is essential for maintaining high standards, supporting employee progression, and ensuring compliance with UK legal and regulatory requirements.

This policy sets out how training will be identified, delivered, recorded, and reviewed across the organisation.

2. Scope

This policy applies to:

- All employees (permanent, temporary, fixed-term, part-time, and full-time)
- Apprentices and trainees
- Agency workers and contractors (where applicable)
- Volunteers (where relevant)

3. Legal Framework

This policy supports compliance with relevant UK legislation and guidance, including but not limited to:

- **Health and Safety at Work etc. Act 1974**
- **Management of Health and Safety at Work Regulations 1999**
- **Equality Act 2010**
- **Employment Rights Act 1996**
- **Working Time Regulations 1998**
- **Data Protection Act 2018 and UK GDPR**
- **Apprenticeships, Skills, Children and Learning Act 2009** (where applicable)

The organisation will also follow best practice guidance issued by ACAS and other relevant regulatory bodies.

4. Policy Objectives

The aims of this policy are to:

- Ensure employees are trained to carry out their duties competently
- Provide mandatory training required by law or regulation
- Promote equality of opportunity in training access

- Support personal development and career progression
- Maintain a skilled, adaptable workforce
- Ensure training is documented and monitored appropriately

5. Responsibilities

5.1 Employer Responsibilities

Cerberus Security Services Limited will:

- Provide training required for employees to perform their roles safely and effectively
- Ensure mandatory legal training is completed and refreshed as required
- Ensure training is accessible and delivered fairly
- Provide reasonable adjustments for disabled employees in line with the Equality Act 2010
- Maintain training records in compliance with UK GDPR

5.2 Manager Responsibilities

Managers are responsible for:

- Identifying training needs through supervision, performance reviews, and operational requirements
- Supporting employees in completing required training
- Ensuring employees are released to attend training during working hours where appropriate
- Monitoring training completion and effectiveness

5.3 Employee Responsibilities

Employees are responsible for:

- Actively participating in required training
- Completing mandatory training within the required timeframe
- Informing their manager of any barriers to training participation
- Applying training in the workplace and maintaining professional standards

6. Types of Training

6.1 Mandatory Training

Mandatory training includes any training required by law, regulation, or company policy, such as:

- Health and safety training

- Fire safety and evacuation procedures
- Manual handling (where applicable)
- Safeguarding (where relevant)
- Data protection and GDPR awareness
- Equality, diversity, and inclusion training
- Anti-harassment and bullying training

Failure to complete mandatory training may result in disciplinary action.

6.2 Role-Specific Training

Role-specific training may include:

- Equipment and machinery training
- Software and systems training
- Customer service training
- Leadership or supervisory training
- Professional qualifications and certifications

6.3 Development and Career Training

Employees may request training to support career progression. Approval is subject to business needs, cost, and relevance to the organisation.

7. Training Requests and Approval Process

Training needs may be identified through:

- Induction
- Probation review
- Annual appraisal/performance review
- Regulatory updates
- Changes in role or operational requirements
- Employee requests

All training requests must be approved by the employee's line manager and, where required, HR or senior management.

Approval decisions will consider:

- Relevance to job duties
- Budget availability
- Operational impact
- Employee performance and development plans

TRAINING AND DEVELOPMENT POLICY

8. Induction Training

All new employees must complete an induction programme which includes:

- Company policies and procedures
- Health and safety requirements
- Equality and diversity standards
- Role expectations and performance standards
- Data protection awareness

Induction should be completed within the first [X] weeks of employment.

9. Equality and Fair Access

Cerberus Security Services Limited is committed to ensuring training is provided fairly and without discrimination.

Training opportunities will be provided in accordance with the **Equality Act 2010**, ensuring no employee is treated less favourably due to:

- Age
- Disability
- Gender reassignment
- Marriage or civil partnership
- Pregnancy or maternity
- Race
- Religion or belief
- Sex
- Sexual orientation

Reasonable adjustments will be made for employees with disabilities or additional learning needs.

10. Time Off for Training

Where training is mandatory or required for the role, it will normally take place during paid working hours.

Where training occurs outside normal working hours:

- Employees will be compensated appropriately (time off in lieu or payment), subject to agreement and Working Time Regulations.
- Travel time may be considered working time depending on circumstances.

11. Payment and Funding of Training

11.1 Company-Funded Training

Where training is approved and required, the organisation may cover:

- Course fees
- Exam fees
- Travel expenses (where agreed)
- Accommodation (where necessary)

11.2 Repayment of Training Costs

Where Cerberus Security Services Limited funds significant external training, a training repayment agreement may apply. This may require the employee to repay some or all costs if they leave employment within a set period (e.g., 6–24 months).

Any repayment agreement will:

- Be reasonable and proportionate
- Be confirmed in writing before training begins
- Comply with the Employment Rights Act 1996 (regarding lawful deductions from wages)

12. Training Records and Data Protection

Training records will be kept by HR and/or management to monitor compliance and development progress.

All training records will be processed in accordance with:

- UK GDPR
- Data Protection Act 2018

Records may include:

- Training attendance
- Certification dates and expiry
- Assessment results
- Development plans

Employees may request access to their training records in line with data protection rights.

13. Monitoring and Evaluation

Training effectiveness will be reviewed through:

- Feedback forms
- One-to-one meetings
- Performance reviews
- Observed workplace performance
- Compliance audits

Where training is found to be ineffective or insufficient, refresher training may be provided.

14. Failure to Attend or Complete Training

Employees are expected to attend training sessions as agreed. Failure to attend without reasonable justification may result in:

- Rescheduling at the employee's expense (where appropriate)
- Formal performance management
- Disciplinary action (especially for mandatory training)

15. External Qualifications and Professional Memberships

Where professional membership or qualification is required for a role, employees must maintain valid registration where applicable.

The organisation may support continuing professional development (CPD) where it benefits the business.

16. Review of Policy

This policy will be reviewed at least every **12 months**, or sooner where changes in legislation, organisational structure, or operational requirements occur.

17. Related Policies

This policy should be read alongside:

- Health and Safety Policy
- Equality, Diversity and Inclusion Policy
- Disciplinary Policy
- Data Protection Policy
- Performance Management Policy
- Recruitment and Selection Policy

Document Retention Policy

1. Purpose

The purpose of this Document Retention Policy is to ensure that [Company Name] retains, manages, and disposes of documents in accordance with applicable UK laws and regulations, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy ensures that documents are:
- Retained only as long as necessary,
- Stored securely,
- Disposed of lawfully and safely,
- Available for audit, regulatory, and business needs.

2. Scope

This policy applies to all employees, contractors, consultants, and third parties who create, process, store, or manage company records in any format, including:
- Paper files,
- Electronic documents,
- Email communications,
- HR and payroll records,
- Financial records,
- Contracts and legal correspondence,
- CCTV and security records.

This policy applies to all company systems including cloud storage, servers, laptops, mobile devices, and third-party storage providers.

3. Legal and Regulatory Framework (UK)

This policy is based on requirements and guidance under UK law, including but not limited to:
- UK GDPR (Retention limitation and data minimisation principles)
- Data Protection Act 2018
- Companies Act 2006
- Limitation Act 1980
- HMRC record-keeping requirements
- Employment Rights Act 1996

Document Retention Policy

- Health and Safety at Work etc. Act 1974
- Equality Act 2010
- VAT Act 1994
- ICO guidance on retention and disposal

Where conflicts exist, the company will apply the longer retention requirement unless legally prohibited.

4. Key Principles

4.1 Retain Only What is Necessary
The company shall not keep personal data or business records longer than required for legal compliance, contractual obligations, business needs, and dispute resolution.

4.2 Secure Storage
All records must be stored securely with appropriate access controls.

4.3 Confidentiality
All documents containing personal, confidential, or commercially sensitive information must be protected from unauthorised access, disclosure, loss, or destruction.

4.4 Timely Disposal
Documents must be disposed of promptly once the retention period expires, unless subject to a legal hold.

5. Responsibilities

5.1 Senior Management
- Approves the policy.
- Ensures resources are available for compliance.

5.2 Data Protection Officer (DPO) / Compliance Officer
- Ensures retention periods comply with UK GDPR and ICO guidance.
- Reviews retention schedules annually.
- Advises on legal holds.

5.3 IT Department
- Maintains secure electronic storage and backups.
- Implements deletion procedures and audit logs.

• Ensures encryption and access control measures.

5.4 All Employees

• Must store company documents only in approved systems.
• Must not retain personal data longer than necessary.
• Must comply with deletion and archiving procedures.

6. Record Storage Requirements

6.1 Paper Records

• Stored in locked cabinets or secure archives.
• Access limited to authorised personnel only.

6.2 Electronic Records

• Stored in approved company systems (SharePoint, secure cloud, internal servers).
• Protected with strong passwords and multi-factor authentication where applicable.
• Regularly backed up and monitored.

6.3 Email Records

Business-related emails must be stored according to retention requirements and not kept indefinitely in inboxes.

7. Retention Schedule (UK Standard Guidance)

The company shall retain documents according to the following schedule (unless a longer period is required by law or contract):

Record Type	Retention Period	UK Legal Reference / Basis
Company statutory records (shareholder registers, resolutions, incorporation documents)	**Permanent**	Companies Act 2006
Annual accounts and financial statements	**6 years minimum**	Companies Act 2006
Accounting records supporting accounts	**6 years**	Companies Act 2006
HMRC tax records (PAYE, corporation tax, VAT)	**6 years**	HMRC requirements
VAT records	**6 years**	VAT Act 1994

Document Retention Policy

Payroll records (PAYE, NI contributions)	**3 years minimum** (recommended 6)	HMRC guidance
Employee personnel files	**6 years after termination**	Limitation Act 1980 (contract claims)
Recruitment records (unsuccessful applicants)	**6–12 months**	UK GDPR (data minimisation)
Employment contracts	**6 years after termination**	Limitation Act 1980
Health & safety accident records	**3 years minimum** (recommended 6)	Health & Safety legislation
Insurance policies and claims records	**6 years after expiry**	Best practice / Limitation Act
Customer contracts and agreements	**6 years after expiry**	Limitation Act 1980
Supplier contracts	**6 years after expiry**	Limitation Act 1980
Litigation and dispute files	**6 years after closure** (or longer if advised)	Limitation Act 1980
Data processing agreements	**6 years after termination**	UK GDPR compliance evidence
CCTV recordings	**30 days** (unless incident occurs)	ICO CCTV guidance
Website logs / access logs	**6–12 months**	UK GDPR necessity principle
Complaint records	**6 years**	Regulatory defence evidence
Policies and compliance documentation	**6 years**	Regulatory audit evidence

8. Special Category Data

Special category personal data (e.g. health data, biometrics, racial or ethnic origin) must be retained only where strictly necessary and with appropriate legal basis.

This data must be stored with enhanced security, including:

- Encryption,
- Restricted access,
- Secure disposal procedures.

9. Legal Holds

Document Retention Policy

Where litigation, audit, investigation, or regulatory review is anticipated or ongoing, the company shall issue a Legal Hold Notice.

During a legal hold:
• Destruction must be suspended,
• Automatic deletion schedules must be paused,
• Employees must preserve all relevant records.

Legal holds remain in place until the Legal Department formally confirms release.

10. Disposal and Destruction

Documents that reach the end of their retention period must be destroyed securely.

10.1 Paper Disposal
• Cross-cut shredding, incineration, or certified destruction services.

10.2 Electronic Disposal
• Secure deletion and wiping (to prevent recovery).
• Removal from backups where technically possible, or marking for deletion during backup lifecycle.

10.3 Destruction Logs
The company must maintain destruction logs for audit purposes, including:
• Document type,
• Date destroyed,
• Method used,
• Authorisation record.

11. Data Subject Rights (UK GDPR Compliance)

Where personal data is retained, the company must ensure compliance with UK GDPR rights including:
• Right of access,
• Right to rectification,
• Right to erasure (where applicable),
• Right to restrict processing.

Document Retention Policy

The company will not delete records required for legal compliance, even if a deletion request is made, but will document the reason for refusal.

12. Breach and Incident Management

Any unauthorised access, loss, or disclosure of documents must be reported immediately in line with the company's Data Breach Policy.

Where required, the company will report breaches to the Information Commissioner's Office (ICO) within 72 hours.

13. Review and Updates

This policy will be reviewed annually, or when there are changes in UK law, ICO guidance, or business operations.

14. Enforcement

Failure to comply with this policy may result in disciplinary action, termination, and/or legal action.

Statutory Sick Pay (SSP) Policy

DISTRIBUTION

This Statutory Sick Pay (SSP) Policy is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

1. Purpose

Cerberus Security Services Limited recognises that employees may from time to time be unable to attend work due to illness or injury. This policy sets out the Company's obligations and arrangements for the payment of Statutory Sick Pay (SSP) in full compliance with the Employment Rights Act 2025 and associated HMRC guidance, incorporating changes that came into effect on 6 April 2026.

This policy does not form part of any employee's contract of employment and may be amended at any time. Any entitlement to Company sick pay beyond the statutory minimum will be set out in the individual employment contract.

2. Scope

This policy applies to all employees of Cerberus Security Services Limited, including full-time, part-time, and zero-hours contract employees, and to qualifying agency workers where statutory entitlement applies. It does not apply to self-employed contractors or individuals who manage their own tax through self-assessment, who are not eligible for SSP.

3. Legal Framework

This policy is based on the following legislation and guidance:

- Employment Rights Act 2025 (SSP provisions effective 6 April 2026)
- Social Security Contributions and Benefits Act 1992
- HMRC Statutory Sick Pay guidance
- Equality Act 2010
- UK GDPR and Data Protection Act 2018

The key changes introduced by the Employment Rights Act 2025, effective 6 April 2026, are:

- **Day-one entitlement:** SSP is now payable from the first qualifying day of sickness absence. The previous three waiting days have been abolished.
- **Earnings limit removed:** The lower earnings limit has been removed. Employees no longer need to earn a minimum weekly amount to be eligible for SSP.

4. Eligibility for Statutory Sick Pay

An employee is eligible for SSP if they:

- Have started work for Cerberus Security Services Limited (i.e. have done some work for the Company);

- Are classed as employed for tax purposes — tax is deducted automatically through PAYE (this includes employees and qualifying agency workers);
- Are unable to work due to illness or injury; and
- Have notified the Company of their sickness within any deadline the Company has set, or within 7 days if no deadline has been specified.

There is no longer a minimum earnings threshold for SSP eligibility. Employees on zero-hours or variable-hours contracts are eligible provided they meet the above criteria. Self-employed workers and those who pay their own tax through self-assessment are not eligible to receive SSP.

5. Statutory Sick Pay — Rate and Payment

When SSP is Paid

From 6 April 2026, SSP is paid from the first qualifying day of sickness absence — a day on which the employee would normally be required to work. For employees with no fixed pattern of work, qualifying days will be agreed between the employee and their manager.

Rate of SSP

SSP is paid at whichever of the following is lower:

- £123.25 per week (the current statutory flat rate); or
- 80% of the employee's average weekly earnings.

Average weekly earnings are calculated based on the 8 weeks immediately before the first day of sickness absence. Payments are rounded up to the nearest penny. SSP is payable for a maximum of 28 weeks in any single period of incapacity and is subject to Income Tax and National Insurance deductions.

Linked Periods of Sickness

Where two or more periods of sickness are separated by 8 weeks (56 days) or fewer, they are treated as a single linked period of incapacity. The average weekly earnings from the first period will be used for all subsequent SSP calculations in that linked period.

Transitional Protection (from 6 April 2026)

Employees who were already receiving SSP before 6 April 2026 and whose average weekly earnings fall between £125 and £154.05 are transitionally protected for the duration of their continuous absence, ensuring their pay is not reduced as a result of the law change. Protection ends on return to work, on completion of 28 weeks of SSP, on leaving employment, or on commencement of Statutory Maternity Pay or Maternity Allowance.

6. When SSP is Not Payable

SSP will not be paid where:

- The employee has already received SSP for 28 weeks in the relevant period;

- The employee is in legal custody;
- The employee is receiving Statutory Maternity Pay, Statutory Paternity Pay, Statutory Adoption Pay, Shared Parental Pay, or Maternity Allowance;
- The absence is due to a trade dispute (other than a lock-out) at the employee's place of work; or
- The employee does not meet the eligibility criteria set out in Section 4 of this policy.

Where an employee is not entitled to SSP, the Company will notify the employee in writing by issuing an SSP1 form (or equivalent letter or email) stating the reason for ineligibility. The employee may then be entitled to claim Employment and Support Allowance or other financial support from the Department for Work and Pensions.

7. Sickness Notification Procedure

Employees who are unable to attend work due to illness or injury must notify their line manager or duty supervisor by telephone on the first day of absence, no later than one hour before their scheduled start time, unless a prior arrangement has been made. Text messages or emails alone are not an acceptable primary method of notification.

Employees must also:

- Provide the reason for absence and expected duration where possible.
- Keep the Company informed of their expected return-to-work date.
- Provide updates if their absence is expected to continue beyond the anticipated period.
- Notify the Company of any change in circumstances that may affect their SSP entitlement.

Failure to follow this notification procedure may result in the absence being treated as unauthorised.

8. Fit Notes and Self-Certification

For absences of 7 calendar days or fewer, employees must complete the Company self-certification form, available from HR or their line manager.

For absences lasting more than 7 consecutive calendar days, employees must obtain a fit note from a registered healthcare professional and submit it to the Company as soon as reasonably practicable. The Company understands that there may be a delay in obtaining a fit note and will take this into account.

Where a fit note indicates the employee 'may be fit for work', the Company will discuss the recommended adjustments with the employee and implement any reasonable measures, which may include a phased return to work, altered hours, amended duties, or workplace adaptations.

9. Return to Work

On returning to work following any period of sickness absence, the employee must inform their line manager or supervisor and complete any required documentation. A return-to-work discussion will be conducted by the line manager or HR for all absences. These discussions are supportive in nature and are designed to facilitate a successful return and to identify any reasonable adjustments required.

10. Long-Term Sickness Absence

Where an employee is absent for an extended period, the Company will maintain regular and reasonable contact with the employee and will seek an occupational health referral where appropriate. Long-term sickness absence will be managed sensitively and in accordance with the Company's obligations under the Equality Act 2010, including the duty to make reasonable adjustments where the condition may constitute a disability.

Where SSP is exhausted after 28 weeks, the Company will issue the employee with an SSP1 form to enable them to claim any applicable state benefits. Any applicable Company sick pay provisions set out in the employee's contract will also be considered at that stage.

11. Record Keeping

The Company will maintain accurate records of all sickness absences and SSP payments in compliance with HMRC requirements, the Company's Document Retention Policy (P-80), UK GDPR, and the Data Protection Act 2018. All records will be held securely with access restricted to those who require it for the administration of this policy.

The following records will be retained:

Record Type	Retention Period	Legal Basis / Reference
SSP payment records (sick pay history)	3 years min (rec. 6)	HMRC / Employment Rights Act 2025
Fit notes / medical certificates	6 years post-termination	Limitation Act 1980
Return-to-work interview records	6 years post-termination	Best practice / Limitation Act
SSP1 ineligibility notices	3 years	HMRC guidance
Absence records / self-certifications	6 years post-termination	HMRC / Employment Rights Act 2025
Linked-period sickness documentation	6 years post-termination	HMRC / Limitation Act 1980

Employees have the right to access their own sickness and SSP records on request, in accordance with the Company's data subject access procedure.

12. Disputes Regarding SSP

If an employee believes they have not received SSP to which they are entitled, or that an incorrect amount has been paid, they should raise the matter in the first instance with HR or their line manager. If the dispute cannot be resolved internally, the employee may contact HMRC's Statutory Payment Dispute Team. The Fair Work Agency, established on 7 April 2026, also holds enforcement powers in relation to statutory sick pay and may be approached where appropriate.

13. Confidentiality

All information relating to sickness absence will be treated as confidential and processed in accordance with UK GDPR and the Data Protection Act 2018. Sickness and absence information will only be disclosed to those who need it to administer this policy or as required by law.

14. Responsibilities

Employees

Employees are responsible for:

- Notifying sickness absence promptly in accordance with Section 7 of this policy.
- Providing self-certification forms and fit notes as required.
- Co-operating with return-to-work discussions and occupational health referrals.
- Informing the Company of any change in circumstances that may affect their SSP entitlement.

Line Managers and Supervisors

Line managers and supervisors are responsible for:

- Recording and reporting all sickness absences accurately and promptly to HR and payroll.
- Conducting return-to-work discussions sensitively and in a timely manner.
- Supporting employees in making reasonable adjustments on return from sickness.
- Referring complex or long-term absence cases to HR without delay.

HR Department

The HR Department is responsible for:

- Administering SSP payments accurately and in accordance with current legislation.
- Issuing SSP1 forms and maintaining accurate, confidential sickness absence records.

- Reviewing and updating this policy to reflect changes in legislation or HMRC guidance.
- Providing advice and guidance to managers and employees on SSP entitlement and procedure.

15. Monitoring and Review

This policy will be reviewed annually by senior management, or sooner following any change to statutory sick pay legislation, HMRC guidance, or Company requirements. The next scheduled review date is June 2027. Employees will be notified of any material amendments and previous versions will be archived.