



Data Protection Policy

SECURITY

Contents

1	Policy Statement	4
2	Purpose	4
3	Scope	5
4	Definitions	6
5	Data Protection Principles	7
6	Lawful Bases for Processing	8
7	Governance and Responsibilities	9
8	Data Subject Rights	11
8.1	<i>Exercising Data Subject Rights</i>	12
8.2	<i>Complaints</i>	12
9	Information Security and Protection of Personal Data	12
9.1	<i>Physical Security Controls</i>	12
9.2	<i>Technical Security Controls</i>	13
9.3	<i>Organisational Security Controls</i>	13
9.4	<i>Information Handling Responsibilities</i>	13
9.5	<i>Continuous Improvement</i>	14
10	Data Classification	14
10.1	<i>Public</i>	14
10.2	<i>Internal</i>	14
10.3	<i>Confidential</i>	15
10.4	<i>Restricted</i>	15
10.5	<i>Classification Responsibilities</i>	16
10.6	<i>Handling and Review</i>	16
11	Data Retention and Disposal	16
12	Personal Data Breach Management	16
12.1	<i>Reporting a Personal Data Breach</i>	17
12.2	<i>Investigation and Assessment</i>	17
12.3	<i>Notification to the Information Commissioner's Office (ICO)</i>	17
12.4	<i>Notification to Affected Individuals</i>	17
12.5	<i>Corrective and Preventative Action</i>	17
13	Data Protection Impact Assessments (DPIAs)	18
13.1	<i>When a DPIA is Required</i>	18
13.2	<i>DPIA Process</i>	18
13.3	<i>Role of the Data Protection Officer</i>	18
13.4	<i>Record Keeping and Review</i>	18
14	Records of Processing Activities (ROPA)	19
14.1	<i>Responsibility for Maintaining Records</i>	19
14.2	<i>Review and Maintenance</i>	19
14.3	<i>Accountability and Compliance</i>	19
15	Third-Party Processors and Data Sharing	19
15.1	<i>Due Diligence</i>	20
15.2	<i>Data Processing Agreements</i>	20
15.3	<i>Security Reviews</i>	20
15.4	<i>Ongoing Monitoring</i>	20
15.5	<i>Data Sharing and Accountability</i>	21
16	International Data Transfers	21
16.1	<i>General Principles</i>	21
16.2	<i>Adequacy Regulations</i>	21
16.3	<i>International Data Transfer Agreements (IDTAs)</i>	21
16.4	<i>Standard Contractual Clauses (SCCs)</i>	21
16.5	<i>Transfer Risk Assessments</i>	22
16.6	<i>Third-Party Providers and Cloud Services</i>	22
16.7	<i>Monitoring and Review</i>	22
17	Training and Awareness	22

17.1	<i>Induction Training</i>	22
17.2	<i>Refresher Training</i>	23
17.3	<i>Specialist Training</i>	23
17.4	<i>Awareness Activities</i>	23
17.5	<i>Training Records</i>	23
17.6	<i>Monitoring and Compliance</i>	23
18	<i>Monitoring, Audit and Continuous Improvement</i>	24
18.1	<i>Internal Audits</i>	24
18.2	<i>Compliance Reviews</i>	24
18.3	<i>Performance Monitoring and Key Performance Indicators (KPIs)</i>	24
18.4	<i>Management Review</i>	25
18.5	<i>Continuous Improvement</i>	25
19	<i>Related Procedures</i>	25

1 Policy Statement

Sentinel Group Security is committed to protecting the privacy, confidentiality, integrity and availability of all personal data processed in the course of its business activities. We recognise that personal information is a valuable asset and that its protection is fundamental to maintaining the trust of our employees, clients, suppliers, contractors, business partners and other stakeholders.

The Company is committed to processing personal data lawfully, fairly and transparently, and to ensuring that appropriate technical and organisational measures are in place to safeguard personal information against unauthorised access, loss, misuse, alteration, disclosure or destruction.

Sentinel Group Security will comply with all applicable data protection and privacy legislation and regulatory requirements, including:

- The UK General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018;
- The Privacy and Electronic Communications Regulations (PECR);
- The Human Rights Act 1998, where applicable;
- Contractual, client and industry-specific data protection requirements;
- Guidance, codes of practice and recommendations issued by the Information Commissioner's Office (ICO).

To demonstrate accountability and compliance, Sentinel Group Security will maintain appropriate governance arrangements, policies, procedures, training programmes and monitoring processes to ensure that personal data is processed responsibly and securely throughout its lifecycle.

All employees, directors, agency workers, contractors, consultants and third parties acting on behalf of Sentinel Group Security are required to comply with this policy and any associated data protection procedures. Failure to do so may result in disciplinary action, contractual sanctions and, where appropriate, legal or regulatory action.

The Chief Executive Officer and Senior Leadership Team are fully committed to promoting a culture of data protection and privacy by design, ensuring that data protection considerations are embedded into business activities, systems, processes and decision-making across the organisation.

2 Purpose

The purpose of this Policy is to establish the framework, responsibilities and controls required to ensure that all personal data processed by Sentinel Group Security is collected, used, stored, shared, retained and disposed of in a lawful, fair and secure manner. This Policy supports the organisation's commitment to protecting the rights and freedoms of individuals whose personal data is processed and to maintaining compliance with applicable data protection legislation and regulatory requirements.

This Policy applies to all employees, directors, temporary workers, contractors, consultants and third parties acting on behalf of Sentinel Group Security who have access to, process, manage or handle personal data in the course of their duties.

The objectives of this Policy are to:

- Ensure compliance with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable privacy legislation.
- Protect the rights, freedoms and privacy of individuals whose personal data is processed by the Company.

- Promote the secure and responsible handling of personal data throughout its lifecycle.
- Reduce the risk of personal data breaches, unauthorised disclosure, loss, misuse or damage to information.
- Establish clear accountability, governance and oversight arrangements for data protection and privacy management.
- Ensure that all employees and relevant third parties understand their responsibilities when processing personal data.
- Maintain the trust and confidence of clients, employees, suppliers, contractors and other stakeholders by demonstrating effective data protection practices.
- Meet contractual, regulatory and customer requirements relating to the management and protection of personal information.
- Support a culture of data protection, information security and privacy by design across all business operations and activities.

Through the implementation of this Policy and associated procedures, Sentinel Group Security seeks to demonstrate accountability, transparency and continual improvement in its management of personal data and privacy risks.

3 Scope

This Policy applies to all personal data processed by Sentinel Group Security, regardless of the format in which it is held, including electronic records, paper records, images, audio recordings, CCTV footage, body worn camera footage and any other information relating to an identified or identifiable individual.

The requirements of this Policy apply to all individuals and organisations acting on behalf of, or under the authority of, Sentinel Group Security, including:

- Employees, whether permanent, fixed-term or part-time;
- Temporary workers and casual staff;
- Agency workers and subcontracted personnel;
- Contractors and freelance workers;
- Consultants and professional advisers;
- Directors and members of senior management;
- Apprentices, trainees and volunteers;
- Third-party suppliers, service providers and data processors who process personal data on behalf of the Company.

This Policy applies to all business activities, locations, systems, applications, devices, databases and records used to collect, store, process, transmit, retain or dispose of personal data. This includes information processed within Company-owned systems, cloud-based services, portable devices, communications systems and any other approved business platforms.

The Policy covers all categories of personal data processed by Sentinel Group Security, including employee information, recruitment records, customer data, supplier information, contractor records and any special category or criminal offence data processed in accordance with legal and regulatory requirements.

All persons subject to this Policy are required to comply with its provisions and with any associated procedures, standards and controls established to support the effective management and protection of personal data. Failure to comply may result in disciplinary action, termination of contractual arrangements and, where applicable, legal or regulatory sanctions.

4 Definitions

Personal Data

Any information relating to an identified or identifiable living individual ("data subject"). An identifiable individual is one who can be identified directly or indirectly by reference to information such as a name, identification number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Special Category Data

Personal data that is afforded additional protection under data protection legislation due to its sensitive nature. This includes information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification purposes, health data, and information concerning an individual's sex life or sexual orientation.

Criminal Offence Data

Personal data relating to criminal convictions, criminal offences, allegations of criminal activity, proceedings relating to criminal offences, or associated security measures. Such information may only be processed where permitted by law and appropriate safeguards are in place.

Data Subject

The identified or identifiable living individual to whom personal data relates. This may include employees, applicants, customers, suppliers, contractors, visitors and other individuals whose personal information is processed by Sentinel Group Security.

Data Controller

The natural or legal person, public authority, agency or other body that determines the purposes for which and the means by which personal data is processed. Sentinel Group Security acts as a Data Controller where it determines how and why personal data is processed.

Data Processor

A natural or legal person, public authority, agency or other body that processes personal data on behalf of a Data Controller. Data Processors may include third-party service providers engaged by Sentinel Group Security to support business operations.

Processing

Any operation or set of operations performed on personal data, whether by automated means or otherwise. This includes collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, using, disclosing, sharing, transmitting, restricting, erasing or destroying personal data.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Consent

A freely given, specific, informed and unambiguous indication of an individual's wishes by which they signify agreement to the processing of their personal data through a clear affirmative action.

Lawful Basis

The legal justification relied upon for processing personal data under UK GDPR, including consent, contract, legal obligation, vital interests, public task or legitimate interests.

Data Protection Impact Assessment (DPIA)

A process used to identify, assess and mitigate privacy risks where processing activities are likely to result in a high risk to the rights and freedoms of individuals.

Records of Processing Activities (ROPA)

The documented record maintained by the organisation detailing its processing activities, including the categories of data processed, purposes of processing, recipients, retention periods and security measures.

Data Protection Officer
(DPO)

The individual appointed by the organisation to provide independent advice on data protection matters, monitor compliance with legislation and policies, and act as a contact point with the Information Commissioner's Office (ICO) and data subjects where required.

These definitions are intended to promote a consistent understanding of data protection terminology and support the effective implementation of this Policy across Sentinel Group Security.

5 Data Protection Principles

Sentinel Group Security is committed to processing personal data in accordance with the principles set out in the UK General Data Protection Regulation (UK GDPR). These principles form the foundation of the organisation's approach to data protection and must be adhered to by all employees, contractors, consultants and third parties who process personal data on behalf of the Company.

Personal data shall be:

- processed lawfully, fairly and transparently. Sentinel Group Security will ensure that personal data is collected and used only where there is a valid legal basis for doing so and that individuals are provided with clear and accessible information regarding how their personal data will be processed.
- collected for specified, explicit and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes. The Company will ensure that the purpose for collecting personal data is clearly defined and documented before processing takes place.
- accurate, complete where necessary and kept up to date. Reasonable steps will be taken to ensure that inaccurate, incomplete or outdated personal information is corrected or deleted without undue delay. Individuals will be provided with appropriate mechanisms to request corrections to their personal data where applicable.
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. Sentinel Group Security will implement and maintain appropriate technical and organisational measures, including access controls, encryption, physical security, staff training and information security controls, to protect personal information throughout its lifecycle.
- retained only for as long as is necessary to fulfil the purposes for which it was collected, or as required by legal, regulatory or contractual obligations. Sentinel Group Security will maintain retention schedules and secure disposal procedures to ensure that personal information is not retained longer than necessary.

Sentinel Group Security will ensure that personal data collected is adequate, relevant and limited to what is necessary for the purposes for which it is processed. The organisation will avoid collecting excessive or unnecessary personal information and will regularly review data collection practices to ensure compliance with this principle.

Sentinel Group Security accepts responsibility for demonstrating compliance with all applicable data protection requirements. The organisation will maintain documented policies, procedures, records, training programmes, audits, risk assessments and governance arrangements to evidence compliance with data protection legislation. Senior management will ensure that sufficient resources and oversight are in place to support effective data protection management across the organisation.

Through the application of these principles, Sentinel Group Security aims to ensure that personal data is processed responsibly, securely and in a manner that respects the rights and freedoms of all individuals.

6 Lawful Bases for Processing

Sentinel Group Security will ensure that all processing of personal data is undertaken in accordance with a valid lawful basis as defined within the UK General Data Protection Regulation (UK GDPR). Personal data will not be collected, used, stored, disclosed or otherwise processed unless an appropriate legal basis has been identified and documented prior to processing commencing.

The Company may rely upon one or more of the following lawful bases when processing personal data:

Consent

Where appropriate, Sentinel Group Security may process personal data based on the individual's freely given, specific, informed and unambiguous consent. Individuals will be provided with the ability to withdraw their consent at any time, and such withdrawal will be respected unless another lawful basis applies.

Performance of a Contract

Personal data may be processed where it is necessary for the performance of a contract to which the individual is a party, or in order to take steps at the request of the individual prior to entering into a contract. This may include employment contracts, supplier agreements or customer service arrangements.

Legal Obligation

The Company may process personal data where it is necessary to comply with a legal or regulatory obligation. This includes, but is not limited to, obligations relating to employment law, taxation, health and safety, safeguarding, law enforcement requests and regulatory reporting requirements.

Vital Interests

Personal data may be processed where it is necessary to protect the vital interests of an individual or another person. This lawful basis is generally limited to situations involving matters of life, death or serious harm where consent cannot reasonably be obtained.

Public Task

Where applicable, personal data may be processed when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation.

Legitimate Interests

Sentinel Group Security may process personal data where it is necessary for the purposes of its legitimate business interests, provided those interests are not overridden by the rights, freedoms or interests of the individual. Where this basis is relied upon, appropriate assessments will be undertaken to ensure that processing is fair, proportionate and compliant with data protection legislation.

Special Category and Criminal Offence Data

Where Sentinel Group Security processes Special Category Data or Criminal Offence Data, the organisation will ensure that, in addition to a lawful basis for processing, an appropriate condition for processing under the UK GDPR and Data Protection Act 2018 has been identified and documented.

Documentation and Accountability

The lawful basis relied upon for each processing activity shall be identified, recorded and maintained within the organisation's Records of Processing Activities (ROPA) and associated privacy documentation. Sentinel Group Security will ensure that lawful basis assessments are reviewed periodically and whenever there is a significant change to the purpose, nature or scope of processing activities.

By identifying and documenting an appropriate lawful basis for processing, Sentinel Group Security demonstrates accountability and ensures that personal data is processed fairly, transparently and in accordance with applicable legal and regulatory requirements.

7 Governance and Responsibilities

Sentinel Group Security is committed to maintaining effective governance arrangements to ensure compliance with data protection legislation and to promote a culture of accountability throughout the organisation. Responsibility for protecting personal data rests with all individuals who process information on behalf of the Company, with specific responsibilities assigned to key roles as outlined below.

Board of Directors

The Board of Directors has overall accountability for ensuring that Sentinel Group Security complies with its legal, regulatory and contractual obligations relating to data protection and privacy. The Board is responsible for:

- Approving and endorsing this Data Protection Policy and associated governance framework;
- Ensuring that sufficient resources, funding and support are available to maintain effective data protection compliance;
- Providing strategic oversight of data protection risks and performance;
- Promoting a culture of privacy, accountability and information security throughout the organisation;
- Reviewing significant data protection risks, incidents, breaches and compliance reports;
- Ensuring appropriate governance arrangements are in place to support compliance with applicable legislation.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for providing independent oversight, guidance and advice on data protection matters and supporting the organisation in meeting its obligations under the UK GDPR and Data Protection Act 2018. The DPO is responsible for:

- Monitoring and assessing the organisation's compliance with data protection legislation, policies and procedures;
- Providing advice and guidance to management and employees on data protection obligations and best practice;
- Reviewing and advising on Data Protection Impact Assessments (DPIAs) and privacy risk assessments;
- Acting as the primary point of contact with the Information Commissioner's Office (ICO) and other regulatory authorities where required;
- Supporting the management, investigation and reporting of personal data breaches;
- Monitoring compliance activities and reporting significant issues to senior management;
- Promoting data protection awareness and supporting staff training and education programmes;
- Responding to data subject requests and privacy-related enquiries where appropriate.

Managers and Supervisors

Managers and Supervisors are responsible for ensuring that data protection requirements are implemented and maintained within the areas under their control. Their responsibilities include:

- Ensuring that employees understand and comply with this Policy and related procedures;
- Implementing appropriate controls to protect personal data within their departments;
- Ensuring that personal data is processed only for authorised and legitimate business purposes;
- Maintaining accurate records and supporting compliance documentation where required;
- Promptly reporting actual or suspected data protection incidents, breaches or risks;
- Supporting investigations, audits and compliance reviews;
- Identifying and addressing data protection risks within operational activities.

Employees, Workers and Contractors

All employees, agency workers, temporary staff, contractors and consultants who process personal data on behalf of Sentinel Group Security have a personal responsibility to protect information and comply with this Policy. Individuals are required to:

- Process personal data only in accordance with authorised business purposes and established procedures;
- Protect the confidentiality, integrity and security of personal information at all times;
- Follow the requirements of this Policy and all associated policies, procedures and standards;
- Report actual, suspected or potential personal data breaches immediately upon discovery;
- Complete mandatory data protection and information security training;
- Cooperate with audits, investigations and compliance activities;
- Ensure that personal data is accurate, secure and handled responsibly throughout its lifecycle.

Failure to comply with this Policy may result in disciplinary action, termination of contractual arrangements, and where appropriate, legal or regulatory action.

All Personnel

Data protection is a shared responsibility. Every individual who handles personal data on behalf of Sentinel Group Security is expected to contribute to the protection of personal information and to support the organisation's commitment to lawful, fair, transparent and secure processing of personal data. Through clear accountability, defined responsibilities and effective governance, Sentinel Group Security aims to maintain the trust and confidence of employees, clients, suppliers and all other stakeholders.

8 Data Subject Rights

Sentinel Group Security is committed to ensuring that individuals are able to exercise their rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The organisation will maintain appropriate procedures and controls to facilitate and respond to requests from data subjects in a timely, transparent and lawful manner.

Individuals whose personal data is processed by Sentinel Group Security are entitled to the following rights:

Right to be Informed

Individuals have the right to be informed about how their personal data is collected, used, stored, shared and retained. Sentinel Group Security will provide clear and transparent privacy information through privacy notices and other appropriate communications to ensure individuals understand how their personal information is processed.

Right of Access

Individuals have the right to request confirmation as to whether their personal data is being processed and, where applicable, obtain access to that information together with details regarding how it is being used. Requests for access to personal data, commonly referred to

as Subject Access Requests (SARs), will be handled in accordance with the organisation's established procedures.

Right to Rectification

Individuals have the right to request that inaccurate, incomplete or outdated personal data is corrected without undue delay. Sentinel Group Security will take reasonable steps to ensure that personal information remains accurate and up to date and will promptly investigate and respond to requests for correction.

Right to Erasure

Individuals have the right, in certain circumstances, to request the deletion of their personal data where there is no lawful reason for its continued processing. Requests for erasure will be assessed in accordance with legal, regulatory and contractual obligations, and may be refused where exemptions apply.

Right to Restrict Processing

Individuals have the right to request that the processing of their personal data is restricted in certain circumstances, for example where the accuracy of the data is contested or where there is a dispute regarding the lawful basis for processing. Where processing is restricted, personal data will only be processed for limited purposes as permitted by law.

Right to Data Portability

Where processing is based on consent or the performance of a contract and is carried out by automated means, individuals have the right to receive their personal data in a structured, commonly used and machine-readable format and, where technically feasible, to have that information transferred to another organisation.

Right to Object

Individuals have the right to object to the processing of their personal data where processing is based on legitimate interests, public task or for direct marketing purposes. Sentinel Group Security will consider all objections and will cease processing where required by law unless compelling legitimate grounds exist to continue the processing.

Rights Relating to Automated Decision-Making and Profiling

Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, where such decisions produce legal effects or similarly significant consequences. Where automated decision-making is used, Sentinel Group Security will implement appropriate safeguards and ensure that individuals are informed of their rights.

8.1 Exercising Data Subject Rights

Sentinel Group Security will establish and maintain procedures for receiving, verifying, recording and responding to data subject requests. All requests will be handled fairly, consistently and without undue delay. The organisation will respond to Subject Access Requests and other applicable data subject rights requests within one calendar month of receipt, unless an extension is permitted under applicable legislation. Where an extension is necessary, the individual will be informed of the reasons for the delay and the expected response period.

8.2 Complaints

Individuals who are dissatisfied with how Sentinel Group Security has handled their personal data or responded to a request may raise their concerns through the organisation's complaints process. If they remain dissatisfied, they have the right to lodge a complaint with the Information Commissioner's Office (ICO) or seek other legal remedies available to them. Through the effective management of data subject rights,

Sentinel Group Security aims to uphold the principles of transparency, accountability and fairness while ensuring individuals retain control over their personal information.

9 Information Security and Protection of Personal Data

Sentinel Group Security is committed to protecting personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, misuse or access. The organisation shall implement and maintain appropriate technical, physical and organisational security measures to ensure the ongoing confidentiality, integrity, availability and resilience of personal data and the systems used to process it.

Security controls will be applied in accordance with the nature, scope, context and purpose of processing activities, together with the risks presented to the rights and freedoms of individuals.

9.1 Physical Security Controls

Sentinel Group Security will implement appropriate physical security measures to prevent unauthorised access to facilities, equipment and information assets containing personal data. These measures may include:

- Secure office premises with controlled access arrangements;
- Visitor management procedures, including visitor registration, authorisation and supervision requirements;
- Lockable storage facilities for paper records and portable devices containing personal data;
- Clear desk and clear screen requirements to prevent unauthorised viewing or access to confidential information;
- Secure disposal facilities for confidential waste and personal data;
- Physical security measures such as locks, alarms, CCTV monitoring and access control systems where appropriate;
- Protection of information assets from theft, loss, damage or unauthorised removal from Company premises.

All personnel are responsible for ensuring that personal data is not left unattended or accessible to unauthorised individuals.

9.2 Technical Security Controls

Sentinel Group Security will implement proportionate technical safeguards designed to protect personal data and reduce cybersecurity risks. Technical controls may include:

- Multi-Factor Authentication (MFA) for systems containing personal or sensitive information;
- Encryption of personal data during transmission and, where appropriate, whilst stored;
- Firewalls and network security controls to protect systems from unauthorised access;
- Anti-malware, anti-virus and endpoint protection technologies;
- Secure password controls and authentication requirements;
- Role-based and least-privilege access controls to restrict access to authorised personnel only;
- System logging, monitoring and audit trails to identify and investigate suspicious activity;
- Regular software updates, patch management and vulnerability management processes;
- Secure backup and recovery arrangements to support business continuity and data restoration;
- Security monitoring and incident detection processes to identify potential threats and vulnerabilities.

Access to systems containing personal data shall be reviewed periodically and removed promptly where it is no longer required.

9.3 *Organisational Security Controls*

In addition to physical and technical safeguards, Sentinel Group Security will maintain organisational measures designed to ensure the secure and lawful processing of personal data. These measures include:

- Mandatory data protection and information security training for all employees and relevant third parties;
- Periodic refresher training and awareness programmes to reinforce security responsibilities;
- Confidentiality agreements, contractual clauses or non-disclosure obligations for personnel with access to personal data;
- Clearly defined policies, procedures and standards governing the handling of personal information;
- Role-based access management to ensure that individuals only have access to the information necessary to perform their duties;
- Risk assessments and Data Protection Impact Assessments (DPIAs) where appropriate;
- Due diligence and security reviews of suppliers, service providers and data processors;
- Internal audits, compliance monitoring and management reviews of security arrangements;
- Incident reporting and breach management procedures to ensure timely identification and response to security events.

9.4 *Information Handling Responsibilities*

All employees, contractors, consultants and third parties processing personal data on behalf of Sentinel Group Security are responsible for protecting information assets and complying with the organisation's information security requirements. Individuals must:

- Handle personal data securely and only for authorised business purposes;
- Prevent unauthorised disclosure of personal information;
- Follow all applicable security policies and procedures;
- Report actual or suspected security incidents immediately;
- Maintain the confidentiality of information accessed during the course of their duties.

Failure to comply with information security requirements may result in disciplinary action, termination of contractual arrangements and, where applicable, legal or regulatory action.

9.5 *Continuous Improvement*

Sentinel Group Security will regularly review and update its information security controls in response to changes in legislation, technology, emerging threats, business requirements and lessons learned from incidents, audits and risk assessments. The organisation remains committed to maintaining effective safeguards that support compliance with data protection legislation and protect the personal data entrusted to it.

10 **Data Classification**

Sentinel Group Security recognises the importance of classifying information according to its sensitivity, value and potential impact in the event of loss, misuse, unauthorised disclosure, alteration or destruction. Information classification enables the organisation to apply appropriate levels of protection and ensure that personal data and business information are handled consistently and securely.

All information created, received, processed or stored by Sentinel Group Security shall be assigned an appropriate classification based on its sensitivity and the level of protection required.

10.1 **Public**

Definition Information approved for public release that may be freely disclosed without causing harm to the organisation, its employees, clients or other stakeholders.

Examples:

- Published marketing materials
- Public website content
- Approved press releases
- Publicly available corporate information

Protection Requirements:

- Information may be shared without restriction once formally approved for release.
- Content must be accurate, current and authorised by the appropriate business owner.
- Public information should be reviewed periodically to ensure it remains appropriate for public disclosure.

10.2 **Internal**

Definition Information intended for use within Sentinel Group Security that is not publicly available but would have limited impact if disclosed unintentionally.

Examples:

- Internal policies and procedures
- Organisational charts
- General business communications
- Operational instructions

Protection Requirements:

- Access should be limited to authorised employees, contractors and approved third parties.
- Information should not be disclosed externally without appropriate authorisation.
- Electronic information should be stored within approved Company systems and locations.
- Appropriate access controls should be applied to prevent unauthorised access.

10.3 **Confidential**

Definition Sensitive business or personal information that could cause harm, financial loss, reputational damage or legal consequences if disclosed to unauthorised individuals.

Examples:

- Employee records
- Customer information
- Supplier contracts
- Financial information
- Personal data
- Commercially sensitive information

Protection Requirements:

- Access shall be restricted to authorised individuals with a legitimate business need.
- Information must be protected using appropriate physical and technical security measures.
- Confidential information must not be shared externally without proper authorisation and, where appropriate, contractual safeguards.
- Electronic transmission should utilise secure communication methods.
- Documents containing confidential information should be securely stored and disposed of when no longer required.

10.4 **Restricted**

Definition Highly sensitive information that requires the highest level of protection due to the significant impact that unauthorised disclosure, loss, alteration or access could cause to individuals or the organisation.

Examples:

- Special Category Data
- Criminal Offence Data
- Data Protection Impact Assessments (DPIAs)
- Security investigations
- Authentication credentials and encryption keys
- Information subject to legal privilege
- Sensitive client or regulatory information

Protection Requirements:

- Access shall be granted strictly on a need-to-know basis and subject to management approval where appropriate.
- Enhanced security controls, including encryption and additional access restrictions, must be applied.
- Storage locations must be secured against unauthorised access.
- Transfer or sharing of restricted information must be authorised, recorded and conducted using approved secure methods.
- Printing, copying or local storage should be minimised and controlled.
- Disposal must be carried out using approved secure destruction methods.

10.5 **Classification Responsibilities**

All employees, contractors, consultants and third parties who create, process or handle information on behalf of Sentinel Group Security are responsible for ensuring that information is correctly classified and protected in accordance with this Policy. Managers and information owners are responsible for determining the appropriate classification level for the information under their control and ensuring that suitable safeguards are implemented and maintained.

10.6 **Handling and Review**

Information classifications shall be reviewed periodically to ensure they remain appropriate throughout the information lifecycle. Where the sensitivity, use or business value of information changes, its classification and associated protection requirements shall be updated accordingly. By implementing a consistent information classification framework, Sentinel Group Security aims to ensure that personal data and business information receive a level of protection proportionate to the risks associated with their processing, storage and disclosure.

11 **Data Retention and Disposal**

Sentinel Group Security is committed to ensuring that personal data is retained only for as long as necessary to fulfil the purpose for which it was collected and to meet legal, regulatory, contractual and operational requirements.

The organisation will ensure that personal data is reviewed periodically and securely disposed of when it is no longer required, in accordance with the principles of storage limitation set out within the UK GDPR.

All employees, contractors and third parties who process personal data on behalf of Sentinel Group Security must comply with the Data Retention Policy and ensure that personal data is retained, archived and disposed of in accordance with approved organisational procedures.

The Director of Compliance and the Data Protection Officer shall oversee compliance with retention and disposal requirements and monitor adherence through periodic reviews, audits and compliance activities

The Data Retention Policy, should be read in conjunction with this Policy.

12 Personal Data Breach Management

Sentinel Group Security is committed to ensuring that all actual, suspected or potential personal data breaches are identified, reported, investigated and managed promptly and effectively in accordance with the requirements of the UK GDPR and Data Protection Act 2018.

A personal data breach may result in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The organisation will maintain appropriate procedures to minimise the risk of such incidents and to ensure an effective and timely response where breaches occur.

12.1 *Reporting a Personal Data Breach*

All employees, contractors, agency workers, consultants and third parties acting on behalf of Sentinel Group Security have a responsibility to report any actual, suspected or potential personal data breach immediately upon becoming aware of it. Examples of reportable incidents include, but are not limited to:

- Loss or theft of personal data or equipment containing personal data;
- Unauthorised access to personal information;
- Accidental disclosure of personal data to an unauthorised recipient;
- Malware, ransomware or cyber security incidents affecting personal data;
- Misdirected emails containing personal information;
- Loss, corruption or destruction of personal records.

Failure to report a known or suspected breach may result in disciplinary action and could increase the risk of harm to affected individuals and the organisation.

12.2 *Investigation and Assessment*

Upon notification of a suspected breach, the Data Protection Officer (DPO) or nominated responsible person shall ensure that an investigation is undertaken without undue delay. The investigation will assess:

- The nature and circumstances of the breach;
- The categories and volume of personal data involved;
- The number of individuals affected;
- The potential impact on affected individuals;
- The likelihood and severity of any risks to the rights and freedoms of data subjects;
- The immediate and long-term actions required to contain, mitigate and remediate the breach.

All breaches, regardless of severity, shall be recorded in the organisation's Data Breach Register, including the details of the incident, actions taken and lessons learned.

12.3 *Notification to the Information Commissioner's Office (ICO)*

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, Sentinel Group Security will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where notification is not made within 72 hours, the reasons for the delay shall be documented and included within the notification to the ICO where appropriate.

12.4 *Notification to Affected Individuals*

Where a personal data breach is likely to result in a high risk to the rights and freedoms of affected individuals, Sentinel Group Security will inform those individuals without undue delay. Notifications to affected individuals will be clear and transparent and, where appropriate, will include:

- A description of the nature of the breach;
- The likely consequences of the breach;
- Actions taken or proposed to address the breach;
- Measures individuals can take to protect themselves;
- Contact details for obtaining further information and support.

12.5 *Corrective and Preventative Action*

Following any personal data breach, Sentinel Group Security will review the circumstances surrounding the incident and implement appropriate corrective and preventative measures to reduce the likelihood of recurrence. This may include improvements to policies, procedures, technical controls, staff training, supplier management arrangements or security measures. The organisation is committed to continual improvement in its data protection and information security practices and will use breach investigations as an opportunity to strengthen compliance and minimise future risk.

13 **Data Protection Impact Assessments (DPIAs)**

Sentinel Group Security is committed to identifying and managing privacy risks associated with the processing of personal data. Where proposed processing activities are likely to result in a high risk to the rights and freedoms of individuals, a Data Protection Impact Assessment (DPIA) shall be completed before the processing activity commences.

A DPIA is a structured process used to assess the necessity, proportionality and risks associated with processing personal data and to identify appropriate measures to mitigate those risks.

13.1 *When a DPIA is Required*

A DPIA must be completed and approved before the implementation of:

- New business systems, applications or platforms that process personal data;
- New technologies, tools or automated processes involving personal information;
- Processing activities that are likely to present a high risk to individuals' privacy rights and freedoms;
- Large-scale monitoring, surveillance or tracking of individuals, including the use of CCTV or other monitoring technologies where appropriate;
- Processing involving Special Category Data or Criminal Offence Data;
- Significant changes to existing systems, processes or services that may affect the handling of personal data;
- New projects, products or services that involve the collection, sharing or use of personal information in a manner that may increase privacy risks.

13.2 *DPIA Process*

The DPIA process shall assess:

- The purpose and scope of the proposed processing activity;
- The lawful basis for processing;
- The necessity and proportionality of the processing;
- Potential privacy and security risks to affected individuals;
- Measures required to eliminate, reduce or manage identified risks;
- Compliance with applicable data protection legislation and organisational policies.

Where appropriate, input shall be sought from relevant stakeholders, including system owners, managers, information security personnel and the Data Protection Officer.

13.3 Role of the Data Protection Officer

The Data Protection Officer (DPO) shall be consulted throughout the DPIA process and will provide advice regarding the assessment of risks, proposed controls and compliance obligations. The DPO shall review completed DPIAs and may recommend additional safeguards where required. Where a DPIA identifies residual high risks that cannot be adequately mitigated, Sentinel Group Security shall consider whether consultation with the Information Commissioner's Office (ICO) is required before proceeding with the processing activity.

13.4 Record Keeping and Review

All completed DPIAs shall be documented, retained and reviewed periodically, particularly where there are significant changes to the processing activity, technology, legal requirements or identified risks. By undertaking DPIAs where appropriate, Sentinel Group Security aims to embed privacy by design and by default into its operations, ensuring that data protection considerations are addressed at the earliest stages of planning and development.

14 Records of Processing Activities (ROPA)

Sentinel Group Security is committed to maintaining accurate and up-to-date Records of Processing Activities (ROPA) to demonstrate compliance with the UK General Data Protection Regulation (UK GDPR) and support the principle of accountability.

The organisation shall maintain documented records of its personal data processing activities and, where required, ensure that such records are available for inspection by the Information Commissioner's Office (ICO) or other authorised regulatory bodies.

The Records of Processing Activities shall include, where applicable:

- The purpose and lawful basis for each processing activity;
- The categories of personal data processed;
- The categories of data subjects to whom the information relates;
- The recipients, third parties or organisations with whom personal data is shared;
- Details of any transfers of personal data outside the United Kingdom and the safeguards applied;
- Applicable retention periods and disposal requirements;
- The technical and organisational security measures implemented to protect personal data;
- The Data Controller and, where relevant, Data Processor responsibilities associated with the processing activity.

14.1 Responsibility for Maintaining Records

The Director of Compliance, Data Protection Officer (DPO), and relevant departmental managers are responsible for ensuring that processing activities within their areas of responsibility are accurately recorded, reviewed and maintained. All departments must notify the DPO of any new processing activities, significant changes to existing processing arrangements, new systems, technologies or data sharing arrangements to ensure that the Records of Processing Activities remain current and accurate.

14.2 Review and Maintenance

Records of Processing Activities shall be reviewed periodically and updated whenever there are changes to the nature, purpose, scope or risks associated with processing activities. Regular reviews will help ensure that:

- Personal data is processed in accordance with documented purposes;
- Appropriate lawful bases have been identified and recorded;

- Retention periods remain appropriate and compliant;
- Data sharing arrangements are accurately documented;
- Security controls remain effective and proportionate to the risks involved.

14.3 Accountability and Compliance

Maintaining comprehensive Records of Processing Activities enables Sentinel Group Security to demonstrate accountability, support effective data governance, facilitate privacy risk assessments and provide evidence of compliance with applicable data protection legislation. The organisation recognises that accurate processing records are a fundamental component of its data protection framework and will ensure that they are maintained as part of its wider governance, risk management and compliance programme.

15 Third-Party Processors and Data Sharing

Sentinel Group Security recognises that, in the course of its business activities, it may engage third-party organisations to process personal data on its behalf. The organisation remains accountable for ensuring that any personal data processed by third parties is protected and handled in accordance with the requirements of the UK GDPR, the Data Protection Act 2018 and any applicable contractual obligations.

Before appointing a third-party processor or sharing personal data with an external organisation, Sentinel Group Security shall ensure that appropriate controls, safeguards and governance measures are in place to protect the information being processed.

15.1 Due Diligence

Prior to engaging a third-party processor, the organisation shall undertake appropriate due diligence to assess the provider's ability to protect personal data and meet applicable legal, regulatory and contractual requirements. Due diligence activities may include:

- Assessment of the processor's data protection and information security arrangements;
- Review of relevant certifications, accreditations and compliance credentials;
- Evaluation of organisational policies, procedures and governance controls;
- Assessment of the processor's capability to meet confidentiality, availability and resilience requirements;
- Consideration of any risks associated with the proposed processing activity.

15.2 Data Processing Agreements

Where a third party processes personal data on behalf of Sentinel Group Security, a written Data Processing Agreement (DPA) or equivalent contractual arrangement shall be established before any processing takes place. Such agreements shall clearly define:

- The nature and purpose of the processing activity;
- The categories of personal data involved;
- The responsibilities and obligations of each party;
- Security and confidentiality requirements;
- Data breach reporting requirements;
- Retention and disposal arrangements;
- Audit and compliance rights;
- Requirements relating to sub-processors and international data transfers.

15.3 Security Reviews

Sentinel Group Security shall ensure that third-party processors maintain appropriate technical and organisational security measures to protect personal data against unauthorised access, disclosure, alteration, loss or destruction. Security reviews may be conducted:

- Prior to the commencement of services;

- During contract renewal activities;
- Following significant changes to services or processing activities;
- Following security incidents, breaches or identified risks;
- As part of routine supplier assurance and compliance programmes.

15.4 Ongoing Monitoring

Third-party processors shall be subject to ongoing monitoring to ensure continued compliance with contractual, legal and security requirements. Monitoring activities may include:

- Regular performance and compliance reviews;
- Assessment of data protection and information security controls;
- Review of audit reports, certifications and assurance documentation;
- Monitoring of incidents, complaints or breaches involving personal data;
- Verification that contractual obligations continue to be met throughout the duration of the relationship.

15.5 Data Sharing and Accountability

Personal data shall only be shared with third parties where there is a lawful basis for doing so and where appropriate safeguards have been implemented. All data sharing arrangements must be proportionate, documented and limited to the information necessary to achieve the intended purpose. The Data Protection Officer (DPO), Director of Compliance and relevant business managers shall oversee third-party processing arrangements and ensure that risks associated with external processing activities are identified, assessed and managed appropriately. Through effective supplier governance, contractual controls and ongoing oversight, Sentinel Group Security aims to ensure that personal data remains protected regardless of whether it is processed internally or by an authorised third-party provider.

16 International Data Transfers

Sentinel Group Security is committed to ensuring that personal data transferred outside the United Kingdom is afforded an adequate level of protection and is processed in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and any applicable regulatory requirements.

Personal data shall not be transferred to, stored in, or accessed from a country outside the United Kingdom unless appropriate safeguards have been implemented to protect the rights and freedoms of individuals and to ensure the security of the information being transferred.

16.1 General Principles

Where international transfers of personal data are necessary for business purposes, Sentinel Group Security shall ensure that such transfers are lawful, transparent and subject to appropriate technical, organisational and contractual safeguards. All international transfers shall be reviewed and approved through the organisation's data protection governance processes prior to implementation.

16.2 Adequacy Regulations

Personal data may be transferred to countries, territories or organisations that have been recognised by the UK Government as providing an adequate level of protection for personal data. Where an adequacy regulation applies, personal data may be transferred without the need for additional transfer safeguards, subject to compliance with all other applicable data protection requirements.

16.3 *International Data Transfer Agreements (IDTAs)*

Where personal data is transferred to a country that is not covered by an adequacy regulation, Sentinel Group Security shall implement appropriate transfer safeguards, including the use of an International Data Transfer Agreement (IDTA) where required. IDTAs shall establish legally binding obligations designed to ensure that personal data continues to receive a level of protection equivalent to that required under UK data protection legislation.

16.4 *Standard Contractual Clauses (SCCs)*

Where appropriate and legally permissible, Sentinel Group Security may utilise approved Standard Contractual Clauses (SCCs) or other recognised transfer mechanisms to support international data transfers. Such contractual measures shall be incorporated into relevant agreements with suppliers, service providers, group entities or other third parties involved in the transfer or processing of personal data outside the United Kingdom.

16.5 *Transfer Risk Assessments*

Before transferring personal data internationally under an IDTA, SCCs or other transfer mechanism, Sentinel Group Security shall undertake a Transfer Risk Assessment (TRA) or equivalent assessment where required. The assessment shall consider:

- The nature and sensitivity of the personal data being transferred;
- The purpose and scope of the transfer;
- The destination country and its legal and regulatory framework;
- The ability of the recipient organisation to protect the information;
- The effectiveness of contractual, technical and organisational safeguards;
- Any risks to the rights and freedoms of affected individuals.

Where unacceptable risks are identified and cannot be appropriately mitigated, the transfer shall not proceed.

16.6 *Third-Party Providers and Cloud Services*

Where cloud service providers, software platforms or third-party processors may store, access or process personal data outside the United Kingdom, Sentinel Group Security shall ensure that appropriate due diligence, contractual safeguards and ongoing monitoring arrangements are in place.

The organisation shall maintain records of international transfers and the safeguards relied upon to support compliance with applicable legal and regulatory requirements.

16.7 *Monitoring and Review*

International data transfer arrangements shall be reviewed periodically to ensure continued compliance with legislative requirements, regulatory guidance and organisational risk management objectives. The Data Protection Officer (DPO), Director of Compliance and relevant business managers shall oversee international data transfer activities and ensure that any changes in processing arrangements, legislation or risk levels are appropriately assessed and managed. Through the implementation of suitable safeguards and risk-based controls, Sentinel Group Security aims to ensure that personal data remains protected regardless of where it is processed or stored and that international transfers are conducted in a lawful, secure and transparent manner.

17 **Training and Awareness**

Sentinel Group Security recognises that effective data protection relies upon all personnel understanding their responsibilities when handling personal data. The organisation is committed to promoting a strong culture of data protection, privacy and information security through ongoing training, awareness and education programmes.

All employees, contractors, agency workers and other individuals processing personal data on behalf of Sentinel Group Security shall receive appropriate training relevant to their role and responsibilities.

17.1 Induction Training

All new employees and relevant third parties shall complete mandatory data protection and information security training as part of their induction process. This training will provide an understanding of:

- Data protection legislation and GDPR requirements;
- Individual responsibilities for protecting personal data;
- Information security expectations and good practice;
- Data breach identification and reporting requirements;
- The organisation's policies, procedures and standards relating to personal data.

No individual should be granted access to personal data or Company systems containing personal information until the required induction training has been completed.

17.2 Refresher Training

To ensure continued awareness and compliance, all personnel shall complete mandatory data protection and information security refresher training on an annual basis. Refresher training will be designed to:

- Reinforce data protection responsibilities;
- Promote awareness of emerging threats and risks;
- Communicate changes to legislation, policies or procedures;
- Share lessons learned from incidents, audits and compliance reviews;
- Support continual improvement in data protection practices across the organisation.

17.3 Specialist Training

Additional role-specific training shall be provided to individuals whose responsibilities involve higher-risk processing activities or enhanced data protection obligations. This may include:

- Managers and Supervisors;
- Human Resources personnel;
- Recruitment teams;
- Compliance and Governance personnel;
- Information Technology and System Administrators;
- Employees responsible for managing data subject requests, investigations or personal data breaches.

Specialist training will focus on the specific legal, regulatory and operational requirements relevant to the individual's role.

17.4 Awareness Activities

Sentinel Group Security will support ongoing awareness through a range of initiatives which may include:

- Policy communications and updates;
- Security awareness campaigns;
- Management briefings;
- Internal guidance materials;
- Lessons learned from audits, incidents and near misses;
- Regular reminders of data protection responsibilities.

17.5 Training Records

Records of all data protection and information security training undertaken by employees and relevant third parties shall be maintained and retained as evidence of compliance. Training records will include, where appropriate:

- Training completion dates;
- Course content and learning objectives;
- Attendance records;
- Assessment or competency results;
- Refresher training requirements.

Managers are responsible for ensuring that personnel within their areas of responsibility complete the training required for their role and maintain compliance with organisational training requirements.

17.6 Monitoring and Compliance

The effectiveness of training and awareness programmes shall be monitored through audits, compliance reviews, training performance metrics and management oversight activities. Additional training may be provided where gaps in knowledge, non-compliance or emerging risks are identified. Through continual training and awareness, Sentinel Group Security aims to ensure that all personnel understand their responsibilities and contribute to the lawful, secure and responsible processing of personal data.

18 Monitoring, Audit and Continuous Improvement

Sentinel Group Security is committed to maintaining an effective data protection management framework through regular monitoring, auditing and review activities. The organisation will assess the effectiveness of its data protection controls, policies and procedures to ensure ongoing compliance with applicable legislation, regulatory requirements and organisational objectives.

Monitoring and assurance activities are designed to identify areas of good practice, address potential risks, support continual improvement and demonstrate accountability under the UK General Data Protection Regulation (UK GDPR).

18.1 Internal Audits

The organisation shall conduct periodic internal audits of its data protection and privacy management arrangements to verify compliance with:

- UK GDPR and Data Protection Act 2018 requirements;
- Organisational policies, procedures and standards;
- Information security controls;
- Data retention and disposal requirements;
- Third-party processing arrangements;
- Data subject rights management processes.

Audit findings shall be documented, reported to relevant management personnel and used to support corrective actions and continual improvement initiatives.

18.2 Compliance Reviews

Regular compliance reviews shall be undertaken to assess the effectiveness of data protection controls and identify any areas requiring improvement. These reviews may include:

- Reviews of processing activities and lawful bases;
- Data Protection Impact Assessments (DPIAs);
- Records of Processing Activities (ROPA);
- Data sharing and international transfer arrangements;
- Personal data breach records and incident trends;

- Training and awareness compliance;
- Supplier and processor compliance assessments.

Where non-conformities or areas of concern are identified, appropriate corrective and preventative actions shall be implemented and monitored to completion.

18.3 Performance Monitoring and Key Performance Indicators (KPIs)

Sentinel Group Security shall establish and monitor appropriate key performance indicators (KPIs) to measure the effectiveness of its data protection programme. Performance indicators may include:

- Data protection training completion rates;
- Number and severity of data protection incidents and breaches;
- Subject Access Request response times;
- Audit findings and corrective action completion rates;
- Compliance review outcomes;
- Supplier assurance and due diligence completion rates;
- Policy review and implementation performance.

Performance data shall be analysed to identify trends, emerging risks and opportunities for improvement.

18.4 Management Review

Senior Management shall periodically review the effectiveness of the organisation's data protection framework to ensure it remains suitable, adequate and effective. Management review activities shall consider, where appropriate:

- Audit and compliance review results;
- Data protection objectives and performance indicators;
- Personal data breaches, incidents and complaints;
- Changes in legal, regulatory or contractual requirements;
- Emerging risks and threats;
- Resource requirements and training effectiveness;
- Recommendations for improvement.

The outcomes of management reviews shall be documented and may result in changes to policies, procedures, controls, resources or organisational objectives.

18.5 Continuous Improvement

Sentinel Group Security is committed to the continual improvement of its data protection and privacy management arrangements. Lessons learned from audits, compliance reviews, incidents, complaints and management reviews shall be used to strengthen controls, improve processes and enhance the protection of personal data. Through effective monitoring, auditing and governance oversight, Sentinel Group Security will maintain a proactive approach to data protection compliance and ensure that the privacy rights of individuals remain appropriately protected.

19 Related Procedures

This Data Protection Policy forms part of Sentinel Group Security's wider information governance and compliance framework and should be read in conjunction with the organisation's supporting policies, procedures, standards and guidance documents.

These documents collectively establish the controls, processes and responsibilities necessary to ensure the lawful, secure and effective management of personal data throughout its lifecycle:

SGS POL 66 Information Security and Technology Policy

SGS POL 41 Data Retention Policy
SGS PRO 21 Data Breach Procedure
SGS PRO 19 Subject Access Request Procedure

Additional supporting documentation may include policies, procedures, standards, guidance notes and operational controls that address specific data protection, privacy, information security or compliance requirements.

All employees, contractors, consultants and third parties acting on behalf of Sentinel Group Security are required to familiarise themselves with, and comply with, all relevant supporting documents applicable to their role and responsibilities.

The Director of Compliance and Data Protection Officer shall ensure that supporting policies and procedures remain aligned with applicable legislation, regulatory guidance and organisational requirements and are reviewed periodically to maintain their effectiveness.

Zafar Chaudhry
Chief Executive Officer
Sentinel Group Security Ltd.

Date: 23rd October 2026