Table of Contents

Introduction

This document outlines the core policies, procedures, and standards that all employees are expected to understand, acknowledge, and follow during their employment with the company. These policies have been developed to promote a safe, respectful, and productive work environment, ensure legal compliance, and support our organizational values and goals.

Each section of this document provides detailed information on specific expectations, including but not limited to conduct, responsibilities, use of company resources, health and safety, ethics, and equal opportunity employment. By adhering to these guidelines, employees contribute to a positive and professional workplace culture.

All employees are required to review this document thoroughly and confirm their acknowledgment of its contents. Failure to comply with any of the policies outlined herein may result in disciplinary action, up to and including termination of employment.

Please note that this document will be reviewed annually and may be updated periodically. Employees will be notified of any significant changes. For any questions or clarification regarding the policies, employees are encouraged to contact their line manager.

Anti-Bribery Policy

Portal Security Ltd requires its staff and other persons who provide or perform a service for or on behalf of PS, at all times to act honestly and with integrity and to safeguard the PS resources for which they are responsible.

PS is committed to ensuring that its business is conducted in an open and transparent manner, will adhere to the six principles of bribery prevention outlined in the Governments guidance, and it will take all appropriate steps to address the risks of bribery.

PS condemns all acts of bribery or corruption; any cases brought to its attention will be investigated exhaustively and dealt with appropriately.

PS is committed to the highest international standards of integrity and to ensuring it adheres to and promotes best practice in bribery prevention.

Bribery is commonly described as the offer or acceptance of a reward to persuade another to act dishonestly and or in breach of the law. It includes the offering,

promising, giving, receiving or soliciting of a financial, or other advantage or favour as a means to influence the actions of an individual (or individuals).

The Bribery Act 2010 provides for 4 bribery offences:

- Bribing: offering, promising or giving an advantage;
- Being bribed: requesting, agreeing to or accepting an advantage;
- Bribing a foreign official;
- Failing as an organisation to prevent any person who performs services on its behalf from committing an act of bribery.

This Policy extends to all PS activities and operations and to all of its dealings and negotiations with third parties in all countries in which staff, and other persons who provide or perform a service for or on behalf of PSS operate. All staff and other persons who provide or perform a service for or on behalf of PSS are required to comply with this policy.

All cases of actual or suspected bribery will be vigorously and promptly investigated and appropriate action will be taken. The police will be informed where considered appropriate.

Disciplinary action will be considered, not only against any staff found to have perpetrated bribery, but also against staff managers whose negligence is held to have facilitated or condoned an act of bribery. Both categories may constitute gross misconduct, the penalty for which may include summary dismissal.

Contract Performance Management

INTRODUCTION

In accordance with BS10800, Portal Security have a written and communicated plan for regular contact with customers.

AIM

To have a process to ensure formal meetings take place with the customer to discuss security service performance, minutes should be taken and records retained.

RESPONSIBILITIES

Mangers will be responsible for implementing the plan at site start up meetings.

APPROACH

- Following a new contract being awarded a site start-up meeting will be arranged.
- The set site start-up agenda will be completed on I-Auditor
- One of the agenda points is frequency of “Client Meeting”
- Client will agree the frequency and meetings will be set using Outlook Calendar

(Construction may be less frequent than corporate)

- Client meeting will be held on the agreed dates.
- The agenda for the meeting will be as follows:
  - Official Client Feedback
  - Monthly Reports Review
  - Incidents
  - Key Performance Indicators
  - Service Level Agreements
  - Aims / Improvements
  - Any Other Business
- Meeting will be recorded on I-Auditor and added to contract file.

Corporate and Social Responsibility Policy

The Management of Portal Security Ltd recognises its Corporate Social Responsibility commitments and its responsibility to work in partnership with members of the security community, employees, suppliers, customers, consumers and wider society.

This commitment is reflected in this policy and in the following policies:

- Quality Policy
- Health & Safety Policy
- Equal Opportunities & TUPE Policy
- Environment Policy
- Data Protection Policy

The elements of which are outlined in each individual policy.

It is the Director’s aim to ensure that; Portal Security Ltd complies with and fully embraces the spirit of the requirements of the QMS. This will enable our company to

maintain, through its adoption, the very highest standards of Customer & Consumer care possible, whilst maintaining and continuously improving the levels of customer/consumer satisfaction and employee development.

This policy statement is understood and followed by all personnel employed by Portal Security Ltd.

Credit Control Policy

This purpose of this policy is to ensure Portal Security Ltd approach late payments in the same way for each of our clients. The importance of cashflow is stressed throughout the business to protect our clients and staff. It aims to bring all outstanding debts to the agreed terms and streamline the cashflow for the business. Portal Security Ltd has a dedicated accounts team supported by a credit controller.

The approach to our credit control policy is:

- Capture, general ledger code and match supporting documents such as a purchase order number and present on invoice.
- Send invoices to authorized approvers to approve or reject invoices.
- Authorize and submit invoices for payment in a financial system.
- Contact customer to make sure they have no queries with invoices they have received and they are on their ledger for payment after 7 days.
- Send statement of account to customer at month end. We may call overdue customers, verbal reminders are believed to be more effective than written ones with every invoice.
- If no payment has been received after 35 days send First reminder to customer.
- Contact Customer with call in between.
- If we still haven't received funds after at 60 days the second chase letter will be sent. If we haven't received payment after 90 days send final chase letter with notice the debt will be passed to Debt collecting agency.

Customer Loss Policy

The purpose of this policy is to outline the procedures for addressing incidents of customer loss and to provide guidelines for offering compensation in the form of credits for CCTV equipment rental or hours worked by Security Operatives.

Portal Security Limited is committed to providing exceptional security services to our clients. In the event of a customer loss, we will review each incident on a case-by-case basis to determine the appropriate course of action. Our goal is to ensure fair and satisfactory resolution for our clients.

The procedure is as follows:

Incident Reporting:

- Clients must report any incidents of loss to Portal Security Limited within 48 hours of occurrence.
- Reports should be submitted in writing, detailing the nature of the loss, date, time, and any relevant supporting documentation.

Incident Review:

- Upon receiving a report, Portal Security Limited will conduct a thorough investigation to assess the circumstances surrounding the loss.
- The investigation will include reviewing CCTV footage, interviewing relevant personnel, and analysing any other pertinent information.

Determination of Compensation:

- Based on the findings of the investigation, Portal Security Limited will determine the appropriate compensation for the client.
- Compensation may be offered in the form of a credit for the rental of CCTV equipment or a credit for the hours worked by the Security Operative involved in the incident.

Notification:

- Clients will be notified of the investigation results and the proposed compensation within 14 days of the incident report.
- If the client accepts the proposed compensation, the credit will be applied to their account accordingly.

Dispute Resolution:

- If the client disagrees with the proposed compensation, they may request a review by contacting Portal Security Limited's Helpdesk.

- A senior manager will re-evaluate the case and provide a final decision within 7 days of the review request.

Data Protection Policy

In compliance with the Data Protection Act 1998.

Data controllers must comply with the provisions of the 1998 Act even if they are exempt from notification.

There are eight Data Protection Principles. In summary they require that data shall be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate
5. not kept longer than necessary
6. processed in accordance with the data subjects' rights
7. secure
8. not transferred to countries outside the EEA without adequate protection.

Diversity and Inclusion Policy

We are committed to fostering a diverse, inclusive, and respectful workplace where everyone is treated with dignity and has equal opportunity to succeed. We recognize that our workforce reflects the communities we serve, and we actively embrace the value that different backgrounds, perspectives, and experiences bring to our team. This policy applies to employees, contractors and applicants for employment and extends to areas of employment, including recruitment, training, promotion, and day-to-day operations.

Portal Security are committed to ensuring fair and inclusive recruitment, selection, and promotion practices; maintaining a workplace culture that respects and values individual differences; providing training and development opportunities that encourage diverse leadership; taking prompt and effective action against any form of discrimination, harassment, or victimisation; ensuring that uniforms, policies, and

communication methods are respectful of cultural and individual identities, while maintaining professional standards; promoting accessibility for all, including people with disabilities or other support needs; and regularly reviewing and improving our practices to reflect evolving standards and expectations.

Employees should recognise any unconscious bias and mitigate its impact; interact respectfully with people of all backgrounds; de-escalate conflicts with cultural sensitivity and empathy; and represent the company with professionalism in diverse social environments.

Senior Management will lead by example, champion this policy and allocate resources to support its implementation. Supervisors and Line Managers will ensure that diversity and inclusion principles are embedded in daily operations. Employees and Contractors are expected to uphold this policy and report any concerns via the appropriate channels. Any employee who feels they have experienced or witnessed behaviour inconsistent with this policy should report it through their Line Manager, or to the Helpdesk. All concerns will be treated seriously, investigated promptly and handled with confidentiality and fairness.

Breaches of this policy may result in disciplinary action, up to and including termination of employment.

Drug and Alcohol Policy

Being under the influence of alcohol or drugs can seriously impair an individual's judgement and reactions leading to an increased risk of accidents and injuries occurring.

The aim of this policy is to ensure the safety of all employees, workers, and visitors by having clear rules in place regarding use and possession of alcohol and drugs, and to support those who have reported a problem with alcohol or drug dependence. Portal Security Ltd. 's alcohol and drugs policy applies to all employees, workers and contractors.

Problems with attendance, misconduct and poor performance in relation to alcohol and drugs will be dealt with in relation to Portal Security Ltd disciplinary procedures.

Portal Security Ltd. 's policy is that during working hours and at all times whilst on work premises employees must be free from the influence of drugs or alcohol. This will help to ensure the health and safety of employees and others with whom they come into contact, to maintain the efficient and effective operation of the business, and to ensure customers receive the service they require.

No employee, worker or contractor shall report or try to report for work when unfit* due to

alcohol or drugs (whether illegal or not) or to substance abuse; be in possession of alcohol or illegal drugs in the workplace; supply others with illegal drugs in the workplace; supply others with alcohol in the workplace, except in the course of work duties. For example serving customers drinks at the bar; consume alcohol or illegal drugs or abuse any substance whilst at work.

*Whether an employee is fit for work is a matter for the reasonable opinion of management.

In addition, employees, workers or contractors must ensure they are aware of the side effects of any prescription drugs; advise their line manager or a member of the management team immediately of any side effects of prescription drugs, which may affect work performance or the health and safety of themselves or others. For example, drowsiness.

Portal Security Ltd will endeavour to ensure that advice and help are made available to any employee who feels they have a problem with alcohol or drug misuse. In the first instance, individuals will be encouraged to seek help from their General Practitioner or attend support groups.

Environmental Policy

Portal Security Ltd (the 'Organisation') recognises the importance of environmental protection and is committed to operating its business responsibly and in fulfilment of its compliance obligations. It is the Organisation's declared policy to operate with and to maintain good relations with relevant regulatory bodies.

It is the Organisation's objective to carry out all necessary activities, to protect the environment and to continually improve the Environmental Management System through the implementation of the following:

- Assess and regularly re-assess the environmental effects of the Organisation's activities
- Training of employees in environmental issues
- Minimise the production of waste
- Minimise material wastage
- Minimise energy wastage

- Promote the use of recyclable and renewable materials
- Prevent pollution in all its forms
- Control noise emissions from operations
- Minimise the risk to the general public and employees from operations and activities undertaken by the Organisation.

Top management demonstrates leadership and commitment with respect to the Environmental Management System by:

- Taking accountability for the effectiveness of the Environmental Management System
- Ensuring that the Environmental Policy and Environmental Objectives are established and are compatible with the strategic direction and the context of the Organisation
- Ensuring the integration of the Environmental Management System requirements into the Organisation's business processes
- Ensuring that the resources needed for the Environmental Management System are available
- Communicating the importance of effective environmental management and of conforming to the Environmental Management System requirements
- Ensuring that the Environmental Management System achieves its intended outcomes
- Directing and supporting persons to contribute to the effectiveness of the Environmental Management System
- Promoting continual improvement
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. The Environmental Policy is communicated to all employees, external providers and other interested parties.

The Policy is regularly reviewed in order to ensure its continuing suitability.

Equal Opportunities & TUPE Policy

Portal Security Ltd wholeheartedly supports the principle of equal opportunities in employment and opposes all forms of unlawful discrimination on the grounds of colour, race, nationality, ethnic or national origin, sex, marital status or disability.

We believe that it is in Portal Security Ltd's best interests, and those of all who work in it, to ensure that the human resources, talents and skills available throughout the community are considered when employment opportunities arise. To this end, within the framework of the law, we are committed, wherever practicable, to achieving and maintaining a workforce which broadly reflects the local community in which we operate.

Every possible step will be taken to ensure that individuals are treated equally and fairly and that decisions on recruitment, selection, training, promotion, and career management are based solely on objective and job related criteria.

Portal Security Ltd undertakes to comply with the Transfer of Undertakings (Protection of Employment) Regulations and preserve employees' terms and conditions when a business or undertaking, or part of one, is transferred to a new employer. Any provision of any agreement (whether a contract of employment or not) is void so far as it would exclude or limit the rights granted under the Regulations.

The equal opportunities policy of Portal Security Ltd has been prepared after due consultation with those involved in its operation, and has the full backing and authority of the Directors.

Health and Safety Policy Statement

Compliance and Commitment Portal Security Ltd commits to ensuring, as far as reasonably practicable, the health, safety, and welfare of our employees and others affected by our operations. We aim to:

- Control risks from work activities.
- Consult with employees on health and safety matters.
- Provide safe working conditions and equipment.
- Provide necessary training and supervision.
- Prevent accidents and health issues.
- Comply with relevant Health, Safety and Fire legislation.

Chief Executive Officer Responsibilities:

- Implement and adapt the health and safety policy as needed.
- Ensure sufficient resources are allocated to meet safety objectives.

Management Responsibilities:

- Prioritise health and safety to prevent injuries and property damage.
- Protect all persons from foreseeable risks.

Employees Duties and Consultation:

- Employees are informed of their duties under this policy.
- Regular consultation with employees to integrate their feedback and improve safety practices.

Systematic Safety Management

We have implemented arrangements to support the effective implementation of this health and safety policy and we commit to:

- Identify hazards, assess risks, and determine control measures.
- Ensure all employees understand and follow the necessary safety procedures.
- Prepare emergency procedures, including evacuation in case of fire or other significant incidents, are clearly set out and communicated to all staff.

We regard all health and safety legislation as setting a minimum compliance standard which we aim to exceed wherever possible and we expect management to achieve their targets without compromising health and safety in any way.

Human Rights Policy

At Portal Security Ltd, we recognize and respect the inherent dignity and equal rights of all individuals. This Human Rights Policy reflects our commitment to upholding fundamental human rights principles in all aspects of our operations.

This policy applies to all employees, contractors, and stakeholders associated with Portal Security Ltd. We expect all parties to adhere to these principles and actively contribute to the promotion and protection of human rights.

Our Core Principles are as follows:

- Non-discrimination

Portal Security Ltd is committed to providing equal opportunities and treatment to all individuals, regardless of race, colour, religion, sex, sexual orientation, gender identity, national origin, disability, or any other protected status.

- Fair Employment Practices

We adhere to fair labour practices, including the prohibition of child labour, forced labour, and any form of human trafficking. We provide fair wages, reasonable working hours, and a safe and healthy working environment.

- Freedom of Association

We respect the right of employees to join or not join trade unions and engage in collective bargaining as allowed by local laws. We encourage open communication and constructive dialogue between employees and management.

- Privacy and Data Protection

We are committed to protecting the privacy and personal data of employees, customers, and other stakeholders. Our data practices comply with applicable data protection laws.

- Health and Safety

Portal Security Ltd is dedicated to providing a safe and healthy work environment. We adhere to occupational health and safety standards and strive to prevent accidents and injuries.

- Environmental Responsibility

We recognize the interconnectedness of human rights and environmental sustainability. We are committed to minimizing our environmental impact and contributing to the well-being of communities in which we operate.

To ensure the effective implementation of this Human Rights Policy, Portal Security Ltd will:

- Communicate this policy to all employees and stakeholders.
- Provide training on human rights principles and their application in the workplace.
- Regularly assess and review our practices to identify and address any potential human rights risks.
- Encourage reporting mechanisms for human rights concerns without fear of retaliation.

- Collaborate with relevant stakeholders to address human rights issues in our supply chain.

Portal Security Ltd is committed to complying with all applicable human rights laws and regulations. We will regularly monitor our performance and seek continuous improvement in our human rights practices.

Inappropriate Relationships Policy

This policy applies to all employees, contractors or individuals working on behalf of, or alongside, the organisation and establishes guidelines for professional conduct concerning personal relationships in the workplace. The purpose is to maintain a respectful, productive and equitable work environment, free from favouritism, conflict of interest and potential harassment.

Employees are often in a position of trust and are therefore expected to conduct themselves in a manner that promotes professionalism and avoids conflicts of interest or the appearance of impropriety. Inappropriate relationships—defined as romantic, sexual, or overly personal relationships—between employees in certain roles may compromise integrity, objectivity, or morale and are therefore subject to restrictions. At all times, employees are expected to maintain professional boundaries and take caution in situations involving power imbalances, where one individual holds a position of authority or influence over another.

The following relationships are strictly prohibited unless properly disclosed and managed:

- Relationships between supervisors and direct reports.
- Relationships between employees and any individual they evaluate or whose work they influence.
- Relationships involving third-party vendors, clients, or partners where there may be a conflict of interest, or a power imbalance.

Any personal relationship where a power imbalance exists is strongly discouraged due to the inherent risk of:

- Perceived or actual coercion
- Favouritism or unfair advantage
- Impaired judgement
- Legal and reputational risks

Employees must understand that consent may not be freely given in relationships involving power imbalances, and such relationships may be subject to greater scrutiny.

Employees engaged in a personal relationship that may present a conflict of interest or power imbalance must disclose the relationship to Head Office. The organisation may take steps to mitigate the situation, including reassignment, adjustment of reporting structures or implementing a formal agreement. Failing to disclose such relationships may result in disciplinary action, up to and including termination.

Reports will be handled with discretion and professionalism. Retaliation against individuals for reporting or disclosing a relationship is strictly prohibited.

Internet Security Policy

The purpose of this ICT Security Policy is to establish guidelines and procedures for safeguarding Portal Security Ltd's information and communication technology resources, data, and systems. This policy applies to all employees, contractors, vendors, and any other individuals or entities with access to Portal Security Ltd's Internet resources.

Portal Security Ltd will classify data into three categories: public, internal, and confidential. Each category will have its own level of security controls.

Access Control includes:

- User Authentication: All users must have unique and strong authentication credentials, including complex passwords and two-factor authentication where applicable.
- Access Rights: Access to ICT resources and data will be granted based on the principle of least privilege. Users will only have access to resources necessary for their job responsibilities.
- Account Management: User accounts will be promptly created, modified, or deactivated in accordance with HR procedures. Former employees' access will be revoked immediately.

Data Security includes:

- Data Encryption: All sensitive and confidential data will be encrypted both at rest and during transmission using industry-standard encryption protocols.
- Data Backup: Regular backups of critical data will be performed, and a disaster recovery plan will be maintained.

Network Security includes:

- Firewalls and Intrusion Detection: Firewalls and intrusion detection systems will be in place to protect the network from unauthorized access and monitor for suspicious activities.
- Network Segmentation: The network will be segmented to isolate sensitive systems and data from the general network, limiting lateral movement in case of a breach.

Endpoint Security includes:

- Anti-Malware: All endpoints will have updated anti-malware and antivirus software installed and regularly updated.
- Patch Management: Operating systems and software will be regularly patched and updated to address known vulnerabilities.

All employees are required to promptly report any security incidents or suspicious activities to the designated IT team. Portal Security Ltd will maintain an incident response plan detailing procedures for identifying, mitigating, and recovering from security incidents.

Regular security awareness and training programs will be conducted to educate employees about security risks and best practices.

Portal Security Ltd will comply with all applicable laws, regulations, and industry standards related to information security, including GDPR, HIPAA, or other relevant standards.

Violations of this policy may result in disciplinary actions, up to and including termination of employment or legal action if warranted.

This policy will be reviewed and updated regularly to adapt to changing security threats and technologies.

Lone Worker Policy

Portal Security Ltd recognises that often our staff will be required to work by themselves for significant periods of time without direct supervision, in isolated work areas and out of hours. The purpose of this policy is to protect such staff so far as is reasonably practicable from the risks of lone working.

The Organisation also recognises it has an obligation under the Health and Safety at Work Act 1974 (HSW Act) and the Management of Health and safety at Work Regulation

1999 (MHSW), for the health, safety and welfare at work of its employees. These responsibilities apply to those staff that, for whatever reason, work alone.

This policy is provided for use of ALL STAFF in their day-to-day work. This policy also covers volunteers and where appropriate, contractors. The policy applies to all situations involving lone working arising in connection with the duties and activities of our staff.

Lone workers are those who work alone without close or direct supervision such as:

i. Staff in fixed establishments where:

- Only one member of staff works on the premises
- Staff working separately from others
- Staff working outside normal hours

ii. Mobile lone workers working away from their base when their work may be carried out in:

- Empty buildings when responding to an alarm e Any sites when on static duty e Gatehouses during non-operational hours
- Response/Patrol vehicles.

It is recognised that any member of staff may spend a limited amount of their working time 'alone'.

The aim of the policy is to: -

- Increase staff awareness of safety issues relating to lone working;
- Ensure that the risk of lone working is assessed in a systematic and ongoing way, and that safe systems and methods of work are put in place to reduce the risk so far is reasonably practicable;
- Ensure that appropriate support is available to staff who have to work alone;
- Encourage full reporting and recording of all incidents relating to lone working; and reduce the number of incidents and injuries to staff related to lone working.

Responsibilities fall as follow:

The Managing Director

- Ensuring that there are arrangements for identifying, evaluating and managing risk associated with lone working;

- Providing resources for putting the policy into practice;
- Ensuring that there are arrangements for monitoring incidents linked to lone working and that these incidents are reviewed along with the effectiveness of this policy.

The Management team, Site Security Supervisors and where appropriate Health and Safety Representatives

- Ensuring that all staff are aware of the policy;
- Ensuring that Risk assessments are carried out and reviewed regularly;
- Putting procedures and safe systems of work into practice which are designed to eliminate or reduce the risks associated with working alone;
- Ensuring that staff groups and individuals identified as being at risk are given appropriate instruction and training, including training at induction, updates and refresher training as necessary;
- Ensuring that the appropriate support Is given to staff involved in any incident;
- Managing the effectiveness of preventative measures through an effective system of reporting, investigating and reporting incidents.

Employees

- Taking responsibility and care of themselves and others affected by their actions;
- Co-operating by following rules and procedures designed for safe working;
- Reporting all incidents that may affect the health and safety of themselves or others and asking for guidance as appropriate;
- Taking part in training designed to meet the requirements of the policy;
- Reporting any dangers or potential dangers they identify or any concerns they might have in respect of working alone.

Risk assessment is essential to good risk management. Assessments shall be carried out for and by all staff whose working practice makes them vulnerable. This includes staff that are site based but work in isolation as well as mobile staff whose work takes them out into the community. Recommendations will be made to eliminate or to reduce the risk to the lowest level reasonably practicable.

In all cases there Is a fundamental question about the need for lone working.

Managers must decide whether systems can be adopted to avoid workers carrying out tasks on their own. If this is not possible the working practice of the member of staff plus other contributory factors must be risk assessed.

Where staff either Work Alone in Buildings or Carry out Site Visits managers should first complete the relevant Lone Workers Checklist.

These checklists can be used as a tool to assist managers to identify if the existing control measures are adequate and If not, what modifications or additional actions can be considered necessary to help reduce the risks associated with Lone Working. The checklists should be retained in the site folder and copy kept at Portal Security Services Ltd main office.

Once the checklist has been completed the manager should carry out a Risk Assessment and document its finding in the location assignment instructions.

Assignment instructions for site based lone workers must include:

- Safe access and exit,
- Risk of violence,
- Channels of communication in an emergency,
- Additional security arrangements i.e. alarm systems, CCTV.

Assignment instructions for response lone workers must include:

- Access to site risk assessments where applicable,
- Procedure for alarm response where applicable,
- Travelling between sites,
- Reporting and recording any incidents of note,
- Communication and traceability
- Personal safety/security.

Following completion of the Risk Assessment, consideration should be given to any appropriate action that is required.

Managers must ensure that risk assessment systems are in place to meet the specific needs of all lone workers within their area of control.

An incident can be defined as an unplanned or uncontrolled event or sequence of events that has the potential to cause injury, ill health or damage. In order to maintain an appropriate record of incidents involving lone workers it is essential that all incidents be reported through the Helpdesk.

Staff should ensure that all incidents where they feel threatened, or 'unsafe' (even if this was not a tangible event/experience) are reported.

This includes incidents of verbal abuse.

If a situation arises which precipitates the need for Police attendance, the employee at risk should contact the on-duty member of the management team. The manger will take the details of the situation and will alert the Police, Site Manager and our response vehicle.

Employees who need assistance from the police whilst in the response vehicle should dial 999 then immediately alert the management team.

The company is actively committed to protecting staff from violence and assault and will support criminal proceedings against those who carry out assault. All staff are encouraged to report violent incidents to the police and will be supported by their manager throughout the process.

Except in cases of emergency, employees should inform their manager of any incidents immediately. The employees' manager will thereafter take responsibility for contacting the Police to report the details of the incident.

All new staff to the company will receive an induction handbook, included in which will be reference to the Lone Workers Policy, and this will be highlighted as part of the employees Induction.

Employees working for the company should know that their safety comes first. Staff should be aware of how to deal with situations where they feel they are at risk, or unsafe. Staff should also be able to recognise how their own actions could influence or even trigger an aggressive response.

Managers will therefore ensure that all lone workers training needs are assessed and that they receive appropriate training.

In the event of a violent incident involving a lone worker, the line manager should immediately ensure that the employee(s) receive any necessary medical treatment and/or advice. If an incident occurs out of hours the on-duty manager/night co-ordinator should be contacted.

Managers should be sensitive to the employee's need to talk about the incident and should take care to avoid any impression that this is not accepted or expected.

Discussion should involve identifying any significant learning points for the employee and other colleagues if necessary. Staff should be made aware that a confidential counselling service can be accessed directly by a member of the management team.

The line manager should also consider whether the employee needs specific information or assistance relating to legal or insurance aspects.

If the employee is a member of a Union or Professional Association he/she may find this an appropriate source of practical and emotional support.

The importance of colleague support should never be underestimated. Colleagues are likely to be seen as primary emotional supports.

The manager should ensure appropriate written and verbal reporting of any violent Incident.

Media Policy

The purpose of this media policy is to establish guidelines for interactions with the media to ensure consistent, accurate, and professional communication that aligns with the values and objectives of Portal Security Ltd.

This policy applies to all employees, contractors, and representatives of Portal Security Ltd.

Only designated individuals are authorized to speak on behalf of Portal Security Ltd. These individuals include:

- CEO
- Directors
- Other individuals specifically designated by the CEO

All media inquiries should be directed to Head Office. Employees should refrain from responding to media inquiries without prior authorization.

All press releases and official statements must be approved by Directors before dissemination. These documents should be clear, concise, and aligned with the company's messaging strategy.

Employees are encouraged to share company news and updates on their personal social media accounts, provided they adhere to the following guidelines:

- Do not disclose confidential or proprietary information.
- Ensure that any shared content is accurate and respectful.
- Include a disclaimer stating that the views expressed are personal and do not represent the company.

In the event of a crisis, Head Office will coordinate all communication efforts. A crisis communication plan will be activated, and only authorized spokespersons will provide information to the media.

Violations of this media policy may result in disciplinary action, up to and including termination of employment.

Modern Slavery Policy

This policy supports Portal Security Ltd's commitment to limiting the risk of modern slavery occurring within our own business or infiltrating our supply chains or any other business relationship.

The policy applies to all persons working for or on our behalf in any capacity, including employees, directors, agency workers, contractors, consultants and any other third-party representatives.

We expect all who have or seek a business relationship with the company to familiarise themselves with this policy and to act always in a way that is consistent with its values.

We will only do business with organisations who fully comply with this policy or those who are taking verifiable steps towards compliance.

This policy will be used to underpin and inform any statement on slavery and human trafficking that we are required to produce further to the transparency in supply chain requirements of Section 54 of the Modern Slavery Act 2015 (MSA).

The MSA covers four key criminal activities:

• Slavery

• Servitude

• Forced and compulsory labour

• Human trafficking

Other forms of modern slavery which will not be tolerated but are not specifically mentioned in the MSA include child labour.

All forms of modern slavery have in common the deprivation of a person's liberty by another to exploit them for commercial or personal gain and amount to a violation of an individual's fundamental human rights. Tackling modern slavery requires us all to

play a part and remain vigilant to the risk in all aspect of our business and business relationships.

Our Service Level Agreement for Suppliers and Contractors contains a specific statement prohibiting slavery or servitude, the use of forced, compulsory or trafficked labour and the use of child labour in line with this policy. We also make provision for our contracted suppliers to hold their own suppliers to the same standards. We also reserve the right to terminate any contractual arrangement if there is breach of this policy.

We have ascertained that our biggest risk in terms of outsourced activities (considering recent research on the construction industry) relates to contractors employed to work at our developments across the country. As such, we have introduced a Toolbox Talk on Modern Slavery to add to our suite of Toolbox Talks which are administered by Site/Estate Managers to site staff. This includes useful information on spotting the signs of modern slavery and labour exploitation such as restricted freedom; behaviour; working conditions; accommodation; finances and appearance.

The Executive Leadership Team has overall responsibility for this policy and in ensuring that the Company complies with all its legal and ethical obligations.

Head Office will have the primary day-to-day responsibility for the implementation of this policy, monitoring its use and ensuring that the appropriate processes and control systems are in place, and amended as appropriate, to ensure it can operate effectively.

All line managers are responsible for ensuring that those reporting directly to them comply with the provisions of this policy in the day-to-day performance of their roles.

Head Office will ensure that all relevant staff receive adequate training on this policy and any supporting processes applicable to their role. Such training forms part of the Company's induction processes as well as Toolbox Talks.

Any breaches of this policy will be taken seriously and dealt with on a case by case basis.

The breach of this policy by an employee, director or officer of the company may lead to disciplinary action being taken in accordance with our disciplinary procedure. Serious breaches may be regarded as gross misconduct and may lead to immediate dismissal further to our disciplinary procedure.

Everybody to whom this policy applies will be expected to co-operate fully in any investigation into suspected breaches of this policy or any related processes or procedures.

If any part of this policy is unclear, clarification should be sought from Head Office. This Anti-slavery policy will be reviewed by the Executive Leadership Team on a regular basis.

This policy does not give contractual rights to company employees and we reserve the right to alter any of its terms at any time. We will notify applicable parties in writing of any changes which may affect them.

Provision of Labour in the Security and Events Sector

This checklist is prepared in accordance with NCP 119.2 – code of practice for the provision of labour in the security and events sector

Company Structure

- Should have a clear management structure
- Should have complaints management system
  - Keep a record of all complaints
  - Take appropriate action in respect of complaints and service deficiencies
  - And document actions taken

Finances

- Should be trading lawfully in UK
- Should have sufficient working capital and reserves to meet all their financial obligations
- Should prepare annual accounts in accordance with applicable accounting standards and have them available for examination upon request

Payroll

- National minimum wage is adhered or exceeded, minimum wage calculations should not include holiday pay, transport, uniform, or other benefits in kind.
- Should adhere to the legislation on statutory holiday pay, auto enrolment to workplace pension schemes for all eligible employees.

- Should comply with all the relevant tax and national insurance legislation concerning people it deploys in accordance with HMRC guidance.
- Staff are paid correctly and on time through a PAYE compliant system with no unlawful deductions.

Insurance

- Should maintain appropriate business insurance, as minimum employer's liability insurance
- All insurance certificates should be directly produced by the insurer with the exact trade being undertaken and cover to a sufficient level to ensure both third parties and staff are properly protected.

Premises

- Should operate from suitable and adequate premises where information relating to staff, suppliers and contractors can securely stored in line with relevant legislation.

Personnel

Selection, right to work and security screening

- Should screen staff in accordance with BS 7858, and certificates should be readily available upon request.
- Should verify staff's right to work in the UK through original documentation and shall made them available upon request.
- Should check the validity of the SIA licence and right to work in the UK for all licensed staff at least monthly

Training

- Should have clearly defined and documented training policy.
- Should provide induction training to all staff in the matters related to employment and procedures including the importance of site-specific AIs and RAMS
- Should maintain records of all trainings undertaken by staff.

Terms and conditions

- Should provide all staff with a ‘written statement of employment particulars’ including
  - Job title
  - Job description
  - Effective start date
  - Probationary period, if required
  - Provisional period subject to screening
  - Employer’s details including address
  - Place of work
  - Pay and allowances
  - Hours and days of work
  - Leave entitlement
  - Conditions of payment during absence through illness
  - Pension entitlement
  - Industrial injury procedures
  - Equipment and uniform supplied
  - Disciplinary and appeals procedures
  - Terms of notice of termination of employment
  - Confidentiality

Uniform

- Should provide uniform to their staff and ensure it is maintained and presentable

Sale of service

Contractual documentation

- Should provide clear information in relation to the services being offered, the information should at least include
  - The terms and conditions under which the work would be carried out
  - The total costing for the service, and the arrangements for payment
  - The contract period, along with procedures for the termination of the contract and reference to any exclusion, penalty clauses or other restrictions
  - The liabilities of the labour provider, which shall not be unlimited, other than by law
  - Details of the contractor's requirements, derived from pre-service discussions or from written instructions, and including clear cross-reference to any separately documented requirements or instructions
  - Arrangement for statutory holidays
  - The obligations of the provider to the contractor, including any provision of specialist advice or duties and reference to any relevant British Standards
  - The obligation of the provider to maintain confidentiality with respect to information obtained whilst tendering for or fulfilling a contract.
  - Any contractor requirement to provide and/or maintain any specified item or service, which is necessary for fulfilling the contractual obligations, including making available to all staff the following site-specific documents:
    - Assignment Instructions
    - Health & Safety Risk Assessment
  - Security screening requirements (including acceptability of full and partial screening)
  - Health and safety arrangements and responsibilities, e.g., provision of staff welfare and lone worker processes, copies of applicable risk assessments.

Contracts

- Should ask contractor to sign either

- An agreement – demonstrating they have read and understood the quotation and terms and conditions of the labour provider; or
- A contract document referring to the quotation and terms and conditions.

- The above should be agreed and exchanged before work commences
- Where requests for services are short notice due to urgent or unforeseen circumstances, contracts should be exchanged as soon as practicable but **no later than 28 days** after the cessation of the cover
- Should changes be required after the quotation and terms and conditions have been accepted by the contractor, these should be agreed in writing with the contractor within 7 days

Operations

Deployment and management of personnel

- Should have a documented health and safety policy and this should be communicated to all staff
- Responsibilities for health and safety should be clearly defined, including provision of welfare facilities and lone worker arrangements as a minimum, including the monitoring of check calls and escalation process for missed check calls

Suppliers

- Should only supply their own staff

Confidentiality

- Staff deployed by labour provider should individually sign confidentiality agreement relating to the non-disclosure of the confidential information and/or material, which should be retained in their personnel file

Documentation/Records

Retention

- Should maintain separate records for each contractor and employee

- The record should be held securely, but easily accessible to authorized persons and retained only for as long as legislation permits with the consideration to the relevant data protection legislation including Data Protection Act and GDPR
- Records relating to the contractual agreement between the contractor and the labour provider should be retained in a contractor file, these records should include pre-contract documentation, agreed service levels and contractor correspondence.
- Archived records should be identifiable and retrievable
- All records concerning a contractor shall be maintained for at least 12 months after termination of the service, such records shall include but not limited to
- Full details of persons deployed on the assignment including screening, licensing, and training
- Correspondence and complaints received from the contractor.
- Basic records for all staff (as detailed in BS 7858) should be kept for at least 7 years from the cessation of their employment.

Quality Policy

Portal Security Ltd (the 'Organisation') aims to provide defect-free products and services to its customers on time and within budget.

The Organisation operates a Quality Management System that has gained ISO 9001 : 2015 certification, including aspects specific to its scope of certification.

The management is committed to:

- Develop and improve the Quality Management System
- Continually improve the effectiveness of the Quality Management System
- The enhancement of customer satisfaction.

The management has a continuing commitment to:

- Ensure that customer needs and expectations are determined and fulfilled with the aim of achieving customer satisfaction
- Communicate throughout the Organisation the importance of meeting customer needs and all relevant statutory and regulatory requirements

- Establish the Quality Policy and to set Quality Objectives at relevant functions, levels and processes
- Ensure that the Management Reviews set and review the Quality Objectives, and report on the internal audit results as a means of monitoring and measuring the processes and the effectiveness of the Quality Management System
- Ensure the availability of resources.

All personnel understand the requirements of this Quality Policy and abide with the contents of the Quality Management System.

The Organisation constantly monitors its quality performance and implements improvements when appropriate.

Sustainability Policy

The purpose of this Sustainability Policy is to outline Portal Security Ltd's commitment to environmental responsibility and sustainability as a provider of security services.

This policy applies to all aspects of our operations, including but not limited to our services, supply chain, facilities, and employees.

Portal Security Ltd is committed to:

- Reducing energy consumption by implementing energy-efficient technologies and practices in our facilities and operations.
- Minimizing waste generation through recycling, reusing, and responsible waste disposal. Our goal is to reduce our environmental footprint.
- Conserving water resources through efficient use and conservation measures in our facilities and operations.
- Working with suppliers and partners who share our commitment to sustainability and environmental responsibility.
- Considering the environmental impact of the products and services we provide and strive to minimize their ecological footprint.
- Reducing our carbon footprint by promoting carpooling, public transportation, and encouraging employees to use eco-friendly modes of transport when possible.
- Where feasible, employees will be encouraged to telecommute or use virtual meetings to reduce travel and associated emissions.

- Engaging with local communities and stakeholders to raise awareness about environmental sustainability and participate in local sustainability initiatives.
- We will consider making charitable contributions to organizations or causes that promote sustainability and environmental conservation.
- Providing our employees with training and resources to help them understand and support our sustainability efforts.

Employees who actively contribute to our sustainability goals may receive recognition and incentives.

Portal Security Ltd will establish key performance indicators (KPIs) to measure progress toward our sustainability goals. Regular reports will be made available to employees and stakeholders.

Senior management will be responsible for the implementation of this policy, and employees at all levels are expected to contribute to sustainability efforts.

Training Policy

Portal Security Ltd is committed to providing the necessary training to ensure our workforce meets the statutory requirements of the Private Security Industry Act 2001. We are also committed to providing the necessary personal development to improve the skills and competence of our workforce in the focused delivery of services to our clients.

The aim of training is to ensure that all employees are given the necessary help to develop the knowledge, skills and attitude they require to carry out their jobs legally and efficiently and to provide every opportunity for career development.

To maintain the structures and mechanisms for identifying training needs and for monitoring the effectiveness of Portal Security Ltd's training policy and programmes.

Operation Manager function will ensure that every member of staff has undertaken and passed the required statutory training before their SIA license application is submitted, if not already in possession of an SIA license at the time of engagement.

The Operation Director is responsible for the continual monitoring of staff training and development throughout the year and to provide the necessary assistance and encouragement to ensure that the company objectives are being met, procedures are being followed and staff's needs are being achieved.

An internal review of Portal Security Ltd's training policy and procedures will be carried out every 12 months.

Training will be delivered in three stages:

Stage 1: Statutory Training

This is the training required to met the statutory requirement of the Private Security Industry Act 2001. Having completed this training an employee will have met the legal standard required for them to become an SIA licensed security officer.

Stage 2: Contract/Site/Client Specific Training

This is the training required to enable an employee to work on a particular contract, site or for a particular client. This will include, but not be limited to, Health and Safety at Work training specific to the contract, site or industry sector. Upon completion of this training the employee will be qualified to work on the contract, site or for the client in question.

Stage 3: Continuation Training and Personal Development

This is the training which further improves the skills and knowledge of the employee and which, amongst other things, will prepare the employee for promotion. This includes personal development training as required under BS7499.

A record of training will be established for each individual employee and held centrally on the personnel file. This will be continually updated throughout the lifecycle of their employment to provide an auditable trail of their training and development. Where the requirements of a contract demand it, a record in the form of a Training Matrix, specific to the contract, may also be kept.

All staff, including new personnel, will have their skills continually assessed by their Contract Manager as identified below:

At the time of recruitment – any immediate training needs identified by the Contract Manager will be addressed prior to commencing work.

At appraisal stage – it is Portal Security Ltd's policy to undertake an annual staff formal / informal appraisal to review performance over the previous twelve months, to identify ways of maximising strengths and improving areas of development in the context of achieving Portal Security Ltd's aims and objectives. These formal / informal reviews are the main vehicle of reviewing and identifying continuation training needs to improve job performance.

At the time of an employee being promoted – covering skills required to equip new managers with the necessary skills to manage staff.

Specific requirements of a project – projects may have unique training requirements that are most appropriately satisfied at project level to ensure the successful delivery of schemes.

Training needs as required as a result of corporate change – which will affect everyone within the organisation.

Training related to professional development. All professional staff are required to comply with the rules of their professional bodies in respect of Continuing Professional Development ("CPD").

The company officer in charge of training will have overall responsibility for analysing training needs identified by the processes above and will discuss with the appropriate Contract Manager and employee the most appropriate and cost effective way of addressing these.

Whistleblowing Policy

At Portal Security Ltd, we are committed to the highest standards of integrity, transparency, and accountability in our operations. This Whistleblowing Policy provides a clear framework for employees, contractors, and stakeholders to raise concerns about any suspected wrongdoing or unethical behaviour within the company without fear of retaliation.

This policy applies to all employees, contractors, consultants, suppliers, and any other third parties associated with Portal Security Ltd. It covers concerns related to illegal activities, misconduct, or any other behaviour that could potentially harm the company, its employees, or the public.

Whistleblowing is the act of reporting any illegal, unethical, or inappropriate conduct within the company. This may include, but is not limited to:

- Fraud, bribery, or corruption
- Theft or misuse of company assets
- Violations of laws or regulations
- Health and safety breaches
- Discrimination, harassment, or bullying
- Environmental damage
- Any other form of misconduct

If you have a concern, you are encouraged to report it as soon as possible. The following steps outline the process:

- Report to Immediate Supervisor: If you feel comfortable, report your concern to your direct supervisor or manager.
- When making a report, please provide as much detail as possible, including: The nature of the concern, the names of individuals involved, the dates and locations of incidents and any supporting evidence.
- All reports made under this policy will be treated with the utmost confidentiality. Portal Security Ltd is committed to protecting the identity of whistleblowers unless disclosure is required by law or necessary for the investigation. Portal Security Ltd strictly prohibits any form of retaliation against individuals who report concerns in good faith. Retaliation includes dismissal, demotion, harassment, or any other adverse action. Any employee found to have retaliated against a whistleblower will face disciplinary action, up to and including termination of employment.
- Upon receiving a report, the Whistleblowing Officer will: acknowledge receipt of the report within five business days, conduct a preliminary assessment to determine if the concern falls within the scope of this policy, initiate a thorough investigation, if necessary, while maintaining confidentiality.
- Keep the whistleblower informed of the progress and outcome of the investigation, where possible.

If the investigation confirms the reported concerns, Portal Security Ltd will take appropriate corrective actions, which may include disciplinary measures, legal action, or changes to company policies and procedures.

While Portal Security Ltd encourages the reporting of genuine concerns, it also recognizes that false or malicious reports can have serious consequences. Any employee found to have made a report in bad faith will be subject to disciplinary action.

Signed: Declan Goldie – *Director*

Issue Date: 01/05/2025

Last Review Date: 01/05/2025

Future Review Date: 01/05/2026

This policy will be reviewed annually or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness. The review will be carried out by the Quality Manager and the date of last review recorded.