An tÚdarás Slándála Príobháidí
The Private Security Authority

PSA LICENSING REQUIREMENTS

Enforcement Guards

Standard for the Licensing of Enforcement Guard Contractors (PSA 91:2023)

www.psa-gov.ie

January 2023

Contents

1. SCOPE

This standard provides a specification for compliance with licensing by the Private Security Authority and applies to contractors seeking a licence to provide security services in the Enforcement Guard sector.

The Government of Ireland through the Private Security Services Act, 2004 as amended, established the Private Security Authority (PSA) as the national regulatory and licensing body for the private security industry. Amongst the functions of the PSA are:

- The controlling and supervising of persons providing security services and maintaining and improving standards in the provision of those services.

- Specifying standards to be observed in the provision of security services.

- Specifying qualifications or requirements for the granting of licences.

Contractors licensed by the PSA and those seeking a licence from the PSA shall comply with this standard. Compliance against this standard will be audited by PSA Inspectors.

Only the most recent edition of the Requirements Document specified by the PSA shall apply for licensing purposes. To ascertain the edition applicable visit the PSA website, www.psa-gov.ie.

2. DEFINITIONS

2.1 **Ancillary Staff.** All security organisation staff not directly employed in duties falling within the definition of Enforcement Guard and Enforcement Manager covered by this standard who may have access to information of a confidential nature.

2.2 **Assessment.** Test carried out to certify the competence of all officers.

2.3 **Auditor**. A person or body appointed by the PSA to provide audit and certification services in respect of the Enforcement Guard sector.

2.4 **Authorised Officials.** Personnel of bodies authorised by statute to enter the premises of the service provider and request documentation and information pertaining to their official functions.

2.5 **Basic Training.** Qualification required by all employees to meet the mandatory training requirements in respect of PSA licensing.

2.6 **Body camera:** A device with audio, video and photographic recording capability that is worn on clothing and is used to record activities by Enforcement Guards or Enforcement Managers

2.7 **Client.** Individual or organisation retaining and maintaining a security service covered by this standard to carry out agreed services in accordance with an agreed contract or other form of oral or written agreement to provide such services.

2.8 **Contract.** Document agreed by both the service provider and the client, setting out the proposed services to be supplied and the details of the quotation, terms, conditions, responsibilities and undertakings.

2.9 **Data Protection Impact Assessment (DPIA).** A process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible.

2.10 **Enforcement Guard.** An Enforcement Guard means a person other than a sheriff, county registrar or court messenger who for remuneration, as part of his or her duties, is authorised to perform any of the following functions:

a) removing one or more persons from any premises or any other place in order to take possession of the premises or place,

b) controlling, supervising or restricting entry by one or more persons to any premises or any other place in order to take possession of the premises or place, or

c) seizing goods or other property in lieu of an outstanding debt,

which said authorisation is conferred by or under an enactment, pursuant to a court order, in accordance with an agreement or a consent, pursuant to a contract, or otherwise in accordance with the law.

2.11 **Enforcement Manager.** A senior person within the organisation responsible for ensuring compliance with all PSA licensing regulations and requirements for the provision of the primary service and who has responsibility for the implementation of the Security Management Plan.

The Enforcement Manager shall be on site when the security service is being provided.

The Enforcement Manager will be considered as a manager of the organisation for the purposes of section 22(3)(b)(i) of the Private Security Services Act.

2.12 **Induction (Training).** The organisation-specific induction briefing session covering organisation structure, ethos, policies and including the organisations and employee's roles and responsibilities.

2.13 **Licence Card.** The official identification card issued by the PSA to each individual employee licence holder to verify his or her licence status. The card to be held on the person of the individual employee whilst providing an enforcement guard service.

2.14 **Organisation**. A body corporate, a partnership or sole trader providing enforcement guard services, for which a relevant and applicable PSA licence is required.

2.15 **Primary Service**. The service, which the organisation and the client have agreed, will be provided, all or part of which will comprise a security service covered by this standard.

2.16 **Principal (of the organisation).** Managing Director, Partner, Majority Owner, authorised member of the Board, Chief Financial Officer, Chief Executive Officer or any person authorised, in writing, by any of these persons to enter into contracts or agreements on behalf of the service provider covered by the provisions and requirements of this standard. A sole trader, for the purposes of this requirements document should be regarded as the principal.

2.17 **Private Security Authority (PSA).** The regulatory and licensing authority for the private security industry in the Republic of Ireland.

2.18 **Relevant Employment.** Employment which involves the provision of a licensable security service or employment which involves, or may involve, the use, acquisition of, or access to, knowledge of a confidential nature, the improper use of which could involve the organisation, its clients, or any third party, in a security risk.

2.19 **Screening.** The selection process and criteria used to check the history and background of potential employees to assist the organisation in its recruitment of new staff covered by this standard.

2.20 **Screening Period.** Period of not less than five years prior to the date of the application for relevant employment or transfer to relevant employment.

2.21 **Security Service.** The provision of a service by a private contractor in the course of their business where all or part of which will comprise a security service.

2.22 **Site:** The premises, property, area or complex at which the security service is carried out.

2.23 **Training Administrator.** A person within the organisation appointed to supervise and record all aspects of training within the organisation.

2.24 **Verification.** Confirmation by sight and written records held at the organisation's premises.

2.25 **Vulnerable Person.** A person, other than a child, who

a) Is suffering from a disorder of the mind, whether as a result of mental illness or dementia,

b) Has an intellectual disability,

c) Is suffering from a physical impairment, whether as a result of injury, illness or age, or

d) Has a physical disability which is of such a nature or degree
    (i) As to restrict the capacity of the person to guard himself or herself against harm by another person or,
    (ii) That results in the person requiring assistance with the activities of daily living including dressing, eating, walking, washing and bathing.

3. ORGANISATION

3.1 Ownership

3.1.1 Ownership and management of the organisation shall be clearly stated in writing. The directors, company secretary and all individuals who have a shareholding or control of more than 5% of the organisation shall be properly identified.

3.1.2 The names of all directors of the organisation shall be properly recorded in the Companies Registration Office, and shall be as named. Screening of all directors shall be carried out as set out in section **4.1**. A record of this screening shall be recorded and held on file, these records shall be available to an authorised official.

3.1.3 Screening shall include details of employment and current and previous directorships, shareholdings etc.

3.1.4 An organisation applying for a licence must provide evidence that they possess the competence to provide a security service. Competence may be demonstrated by the following means:

a) 5 years continuous experience in the sector for which a licence is sought within the previous 8 years, or
b) possession of a PSA contractor licence in the event security, security guarding or door supervision sectors for the previous 5 years, or
c) such other means as may be approved by the PSA.

Note: *Where an organisation is a body corporate, at least one director should demonstrate that they possess the required competence. Where an organisation is a partnership, at least one partner should demonstrate that they possess the required competence, all sole traders should demonstrate that they possess the required competence.*

3.1.5 Details of former businesses, directorships, partnerships, or sole trades etc. of directors shall be recorded and held on file, these records shall be available to an authorised official.

3.1.6 Details of any bankruptcy whether discharged or undischarged of a principal or director of the organisation shall be held on file and shall be disclosed to a client on request.

3.1.7 Where a principal has a beneficial interest in another organisation subject to licensing by the PSA, a declaration of that interest shall be made.

3.1.8 All principals shall sign a declaration providing details of any person who is a beneficiary of the organisation or any person that may hold a major interest in the organisation and who has not been identified at section **3.1.1 or 3.1.2**.

3.1.9 The principal shall ensure that an up to date organisation chart is prepared which details all the persons involved and all persons proposed to be involved in the organisation. The chart shall include details of any third party who will provide additional services to or for the organisation such as sales, payroll and accounts.

3.1.10 All directors, management, supervisory and operational staff shall hold a current PSA employee licence where they are carrying out an activity that is subject to PSA licensing.

3.2 Finances

3.2.1 The organisation shall be tax compliant. Holders of eTax Clearance certificates shall provide the Tax Reference Number (TRN) and Tax Clearance Access Number (TCAN) and allow Authorised Officials access to Revenue.ie to allow verification.

Where access to the Revenue On-line System (ROS) is carried out by an agent, organisations shall provide in addition to the above an up to date ‘hard copy’ of the certificate, the date it was printed showing at the bottom of the document.

3.2.2 Loans from directors and/or shareholders shall be loan capital, subordinated to all other creditors.

3.2.3 Each organisation shall produce and make available, a projected cash flow statement for the next 12 months upon request by authorised officials. For new organisations, a cash flow forecast for the first 12 months of business shall be provided. (see **Annex C** for suggested format).

3.3 Insurance

3.3.1 Organisations are required to hold insurance relevant to the nature of the business undertaken. This includes, where the service provided dictates, but is not limited to cover for the following:

- Employer liability and public liability
- Motor insurance
- Professional indemnity
- Deliberate act
- Fidelity
- Defamation
- Efficacy
- Loss of keys and consequential loss of keys
- Wrongful arrest
- Personal Attack
- Death in Service

3.3.2 The organisation shall have sufficient funds to cover three times the value of the insurance excess amount of their insurance policy. These funds shall be held in a bank account separate to the organisation's operational account.

3.3.3 Organisations shall not self-insure in whole or in part for the services they provide.

3.4 Premises

3.4.1 The organisation shall have an administrative office where records, together with all professional and business documents, certificates, correspondence and files necessary to the proper conduct of business shall be kept in a secure confidential manner.

3.4.2 Any administrative office covered by **3.4.1** above shall be protected by an intruder alarm system installed and maintained in accordance with prevailing PSA requirements. The organisation shall keep a written record containing the name, address, contact number and PSA licence number of the intruder alarm installer as well as details of the maintenance and service history.

3.4.3 The alarm shall be remotely monitored by:

a) a PSA licensed Alarm Monitoring Centre. (The organisation shall keep a written record of the name, address, contact number and PSA licence number of the PSA licensed Alarm Monitoring Centre providing this service) or,
b) such other means as may be approved by the PSA

3.5 Organisation Information

3.5.1 The organisation shall clearly state its PSA licence number(s) for all categories for which it is licensed to provide services on all organisational letterheads, contracts and advertising and promotional documents and/or media.

3.5.2 The provision of contracts to clients is mandatory and contracts shall include the following minimum provisions in respect of the organisation providing the service:

a) Total costing (including VAT) for the service to be provided and the arrangements for payment.
b) Obligations to the client, with references to any specialist advice to be provided (survey), contracted duties (assignment instructions) and compliance with industry standards or codes of practice.
c) Agreement on conditions for the use of subcontractors, where applicable.
d) Period of the contract and requirements for its termination with specific reference to any exclusions, penalty clauses or other restrictions.
e) Safety statement.
f) Details of complaints procedures and complaints management procedures.
g) The scope of the service to be provided.

3.5.3 The agreed contract shall be signed by a principal of the organisation and of the client and a copy retained by each. Where the client chooses not to sign or return a contract the organisation shall maintain evidence on file of postage (registered) or delivery of the contract to the client and any subsequent correspondence.

3.5.4 Organisations engaging subcontractors for any licensable activity in the provision of services shall require the subcontractor to provide evidence of compliance with PSA standards. In addition, subcontractors shall provide evidence of holding the required, current valid PSA licence before the services of that subcontractor are engaged.

3.6 Quotations in pursuance of Contracts or Business

3.6.1 Organisations shall provide each prospective client with a clear written quotation which shall, if agreed and accepted, form part of the contract.

3.6.2 The documented quotation shall include the total cost for the service and method(s) of payment.

3.7 Compliance with Legislation

3.7.1 The organisation shall have and make available to a client or potential client a statement signed and dated by a principal of the organisation, of its compliance with all relevant legislation and shall state specifically its compliance, where relevant, with the following:

- Safety, Health and Welfare at Work Act(s).
- Organisation of Working Time Act(s).
- Private Security Services Acts.
- Taxation and Social Welfare Acts.
- Payment of Wages Act.
- Immigration Acts.
- Data Protection Acts.
- Irish Human Rights and Equality Commission Act 2014.

Relevant verification shall be available to all statutory bodies and their agents, including but not limited to:

- The Private Security Authority.
- Auditors appointed by the Private Security Authority.

3.7.2 The organisation shall appoint a member of the management team responsible for ensuring that the organisation at all times operates in accordance with the provisions of the Private Security Services Act, regulations thereunder and the standards prescribed for licensing.

4. STAFFING

4.1 Selection and Pre-Employment Screening

4.1.1 General

4.1.1.1 The organisation shall carry out detailed pre-employment enquiries to ensure that all personnel are competent and of good character.

4.1.1.2 All persons offered employment by the organisation for posts involving services subject to licensing by the PSA or posts involving access to details of clients shall be screened.

4.1.1.3 A personnel file shall be established for each person subject to screening.

4.1.1.4 All applicants for relevant employment shall be required to provide the following:

a) An acknowledgement signed and dated by the applicant, that misrepresentation, or failure to disclose material facts may constitute grounds for dismissal.

b) A signed statement authorising an approach to former employers, State institutions, personal referees, etc., for verification of their career and employment record (see **Annex A, Form 1** for a suggested format).

4.1.1.5 No applicant shall be offered relevant employment unless they hold a PSA Licence and until screening is completed.

4.1.1.6 Probationary employment should be for a period of six months and in no case shall exceed a period of nine months.

4.1.1.7 Certified copies of all relevant personnel and screening documentation shall be held on file.

4.1.1.8 The requirements in Section **4.1** shall be applied equally to full-time and to part-time employees and at all levels of seniority, including directors.

4.1.1.9 The relevant provisions of these requirements shall apply to all ancillary staff including those employed on a temporary basis.

4.1.1.10 The screening period shall not be less than five years or from school leaving, whichever is the shorter duration.

4.1.1.11 Persons employed for security duties as Enforcement Guard personnel shall not be less than 18 years of age.

4.1.1.12 Persons beyond sixty-six years of age employed for security duties as Enforcement Guard personnel shall be required to undergo an annual medical examination to ensure their fitness for the duties to which they may be assigned.

4.1.1.13 The employee shall be classed as 'employed subject to satisfactory screening' whilst screening is continuing and shall be subject to a strict system of monitoring and supervision during this period.

4.1.1.14 Screening covering the whole of the screening period shall be completed no later than ten weeks after employment has commenced.

4.1.1.15 Full screening for the period covered under **4.1.1.10** above shall apply. Screening for a shorter period can be carried out where:

a) an employee or director holds a current PSA licence, and

b) has, immediately prior to the commencement of this employment, been employed by another licensed security provider, and

c) the previous employer referred to in b) has carried out the full screening requirements within the preceding five years.

Where a), b) and c) above apply, screening shall be carried out from the date the screening by the previous employer had been conducted until the commencement of this employment.

4.1.1.16 Where the provisions of **4.1.1.15** apply, the previous licensed employer shall, upon receipt of a written request by an immediately subsequent employer covered by this standard, forward those parts of the employee’s personnel file relating to details of screening and training undertaken by the previous employer. Any requested details in relation to other parts of the personnel file held by the previous employer shall be released only where the employee gives permission in writing to the previous employer to release such details.

4.1.2 Pre-Employment Interview

4.1.2.1 Prior to the interview the applicant shall submit a curriculum vitae or other documentation containing:

a) A list of the applicant's previous employers along with dates worked for each employer.
b) Contact details for previous employers listed.
c) Details of relevant training, qualifications and experience together with supporting documentation.
d) Periods of unemployment.
e) Applicant's current place of residence.

4.1.2.2 A personal interview of a duration sufficient to assess the following shall be conducted by the organisation:

a) The general ability, both physical and intellectual of the applicant and the overall demeanour of the applicant.
b) Verification of personal documents e.g. birth certificate, driving licence, passport, service records, current security licence, work visa etc.
c) The applicant’s previous employment history and experience, including reason(s) for leaving previous employments.
d) Verification of qualifications/training.
e) The level of occupational fluency in respect of reading, writing and oral communication in the English language.
f) The applicant’s experience, if any, in the security industry.

4.1.2.3 Interview notes evidencing that the requirements set out in **4.1.2.2** above have been addressed shall be taken by the organisation and retained on the personnel file of the applicant.

4.1.3 Character and Other References

4.1.3.1 Screening procedures shall include direct reference to former employers, educational authorities, etc., with confirmation by them, in writing, of periods of employment contributing to a continuous record of the career or history of the person being screened for the whole of the screening period, on a month-to-month basis. The direct reference shall include at least one attempt, in writing, by the organisation to obtain the continuous record referred to in this requirement. Where no response is received to the request for information the requirements set out in **4.1.3.5** shall apply.

4.1.3.2 Where initial references are taken by telephone the following procedures shall be used:

a) The telephone number of the person called shall be confirmed independently.
b) Information given on the telephone by a referee shall be noted at the time of making the telephone call and shall be signed and dated by the member of staff making the telephone call and retained on the individuals screening file (see **Annex A, Form 2** for a suggested format).
c) A written request shall be forwarded to the referee within two working days of the telephone call being made seeking written confirmation of the information provided (see **Annex A, Form 3** for a suggested format).
d) The screening process shall not be regarded as complete until written evidence is obtained.
e) The progress sheet shall be used to monitor and record the action taken (see **Annex A, Form 4** for a suggested format).

4.1.3.3 Only documents from third parties such as employers, colleges, Department of Social Protection, solicitors, accountants are acceptable for screening purposes.

Note. *For the purposes of this document CVs or other personal documents are not acceptable as evidence of screening.*

4.1.3.4 Where records are not available, the period for which the record is not available shall be treated as a gap.

4.1.3.5 Where there are gaps in the career record which cannot be independently confirmed in accordance with the written verification procedures, the following procedure shall be followed:

a) Written statements from personal referees shall be used, provided they had personal knowledge of the person being screened on a month-to-month basis during the period covered.
b) The organisation shall be satisfied as to the creditability of the personal referee.
c) The written statement shall as a minimum confirm that the applicant was where he/she purported to be and may, subject to the credibility of the referee, include a character reference.

d) A progress sheet shall be used to monitor and record the action taken.

Note. *For the purposes of this document personal referees shall not include family members, work colleagues or friends.*

4.1.4 Evidence of Qualifications/Awards

4.1.4.1 Prior to commencement of employment the organisation shall ensure that the applicant has any qualifications or awards necessary for the duties to which the applicant will be employed.

4.1.5 Work Permits, Authorisations and Permissions

4.1.5.1 The organisation shall ensure that all necessary documentation for work visa applications and permissions/authority to work is fully completed before the individual is employed. This applies to renewal of such applications also.

4.1.5.2 The organisation shall maintain a register of all employees who have applied for and obtained permission or authorisation from the State to work in Ireland. The organisation shall review the validity of these permissions or authorisations at least every 6 months and shall keep a documented record of such reviews.

4.1.5.3 The organisation shall ensure that the register at **4.1.5.2** is held on site at the address recorded on the Private Security Services Licence.

4.1.6 Maintenance and Retention of Records

4.1.6.1 The basic details of the employee, covering verifiable history within the industry, dates employed, positions held, disciplinary offences and a comment on suitability for employment in the security industry shall be retained for not less than five years from the date the employment ceases. This information shall be verifiable in the form of readily retrievable records held at the organisations premises.

4.1.6.2 All records covered by **4.1.6.1** above shall be kept safe and secure against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Employers shall ensure that the records are retained for no longer than is necessary and in accordance with the recommendations of the Data Protection Commission.

4.1.6.3 A list of all personnel currently employed both on a permanent and a probationary basis shall be maintained. In the case of those employed on a probationary basis, the dates on which probationary employment commenced and is to cease for each individual shall be recorded.

4.1.7 Screening and Acquired Companies

4.1.7.1 Where it cannot be established by the records of an acquired organisation that screening to the required standard has already occurred, then this shall take place within a period not exceeding thirteen weeks from the date of acquisition.

4.2 Terms of Employment

4.2.1 All employees shall receive a clear, concise and unambiguous contract of employment and a staff handbook.

4.2.2 In addition to any mandatory requirements, terms of employment shall include the following information:

a) Job title.
b) Effective start date.
c) Probationary period.
d) Pay and Allowances.
e) Hours of work, days of work, shift frequency and shift variables.
f) Holiday entitlement.
g) Sick pay (conditions of payment) and pension entitlement.
h) Industrial injury procedure.
i) Location of place of work (employer’s address).
j) Equipment to be supplied.
k) Disciplinary and grievance procedures.
l) Terms of notice and termination.
m) Copies of any Collective Agreement covering the employment.
n) Appeals procedure.
o) The Organisation's Health and Safety Statement.
p) The Organisation's Equality policy.

4.3 Code of Conduct

4.3.1 All employees shall be instructed that under the terms and conditions of employment they shall:

a) Complete the required tasks promptly and diligently, unless there is due and sufficient cause not to.
b) Ensure that all oral or written statements made by them, of whatever description, are true and accurate.
c) Maintain carefully all documents and ensure that any alterations, disposal, or erasure of documents is carried out only with proper authorisation.
d) Maintain confidentially on any matter relating to the employer or his clients either past or present.
e) Ensure that any actions taken by them are such as not to bring discredit on the employer, the client or fellow employees.
f) Immediately notify any conviction for a relevant criminal or motoring offence to the employer.
g) Not allow unauthorised access to a client's premises.
h) Ensure that they use employer's equipment or facilities only with authorisation.
i) Continuously satisfy the requirements of PSA licensing.
j) Hold on their person a PSA licence card at all times whilst on duty.

4.3.2 The code of conduct shall be signed by all employees.

4.3.3 Employers shall treat employees with courtesy and respect.

4.4 Licence Card

4.4.1 The organisation shall ensure that all Enforcement Managers and Enforcement Guards have a valid PSA licence card.

From the 31st March 2023 until the 31st March 2024, Enforcement Managers and Enforcement Guards should hold a PSA Door Supervisor or a PSA Security Guard licence.

Note: *The PSA is currently developing a training course specific to enforcement guards. The new course will become the training requirement for enforcement guard licensing. The PSA expects to commence enforcement guard licensing for employees on the 31st March 2024.*

4.4.2 All employees shall be instructed on PSA requirements relating to the use of their licence card.

4.5 Uniform

4.5.1 The organisation shall provide each Enforcement Manager and each Enforcement Guard with an identical style of outer clothing, in this standard referred to as the uniform. The uniform shall remain the property of the organisation.

4.5.2 The uniform shall include colouring and lettering so to be readily distinguishable from the public and in a crowd. The uniform shall be green.

Lettering clearly indicating the word “ENFORCEMENT GUARD” shall be placed on the front left breast and the word “ENF. GUARD” on the back of the uniform and both should be clearly visible from a distance of 15 meters.

The word “ENFORCEMENT GUARD” shall be in uppercase letters and be not less than 1.5 centimetres high on the front left breast of the uniform. The word “ENF. GUARD shall be not less than 10 centimetres high on the back of the uniform. All lettering shall be permanently affixed to the uniform.

Note: *All personnel wearing the uniform will be regarded as enforcement guards for PSA purposes.*

4.5.3 The uniform shall be readily distinguishable from that of a member of the civil protection services.

4.5.4 Each uniform shall contain a unique identity number on the front and back. The unique identity number shall be not less than 7 centimetres high and shall be clearly visible when the uniform is worn in normal working environments.

4.5.5 The uniform shall display insignia identifying the organisation providing the service and the wearer as an organisation employee. The organisation's insignia shall be clearly visible when the uniform is worn in normal working environments.

4.5.6 All personnel wearing the uniform shall ensure that their facial features are clearly visible at all times. The wearing of head coverings are only acceptable for religious reasons.

4.5.7 Subject to normal wear and tear the organisation shall provide for the renewal of uniforms.

4.5.8 The cost of the uniform shall be borne by the organisation.

4.5.9 Where an employee leaves an organisation and the uniform is not returned to the organisation, the cost of the uniform may be deducted from any payment due to the employee.

4.5.10 A record of all uniforms not returned shall be retained by the organisation. The record shall contain the name of the employee, their PSA licence number and the unique identity number of the uniform,

5. TRAINING

5.1 Training Policy and Responsibility

5.1.1 The organisation shall have a clearly defined, documented training policy, authorised at senior management level within the organisation. The policy shall cover theoretical and practical skills and meet any training requirements laid down by the PSA.

5.1.2 The organisation shall appoint a member of the management team as training administrator.

5.1.3 The organisation shall ensure that all relevant staff meet the training requirements prescribed by the PSA.

5.1.4 The training policy shall include a commitment to assess the effectiveness of all operational staff and to provide additional training where required.

5.2 Induction Training

5.2.1 Training shall include a detailed organisation-specific, induction session covering organisation structure, ethos, policies and employee roles and responsibilities for all newly recruited employees. This element of training shall be delivered before the employee commences operational duties. The training shall ensure that the employee understands and is able to act, at all times, professionally and within the bounds of the relevant legislation. Each employee shall acknowledge receipt of this training and associated documentation by signing a declaration. Such training shall be delivered by a competent member of staff and shall be recorded and this record shall be retained.

5.3 Specialist Training

5.3.1 Employers shall ensure that employees required to carry out duties or use equipment of a specialist nature are certified as having received the appropriate training in the subject matter.

5.3.2 Where risks are identified, in the course of carrying out a risk assessment, additional training, specific to these risks, shall be provided where training has not previously addressed the nature of the risk(s) involved.

5.4 Refresher Training

5.4.1 Procedures shall exist to assess the effectiveness of all employees, and where required refresher training shall be carried out.

5.5 Supervisory and Management Training

5.5.1 Subject to PSA requirements and any associated guidelines, the organisation shall ensure that all operational supervisory and management staff receive documented training in consideration of their position and responsibilities.

5.6 Training Records

5.6.1 The training administrator shall ensure that proper training records are maintained.

5.6.2 Individual training records relating to training provided by the organisation shall indicate the date, training organisation, details of certification and subject(s) covered. These training records shall be signed by the employee and countersigned by the training administrator and retained as part of the employee's record.

5.6.3 Verification of all training shall be available for inspection at the address recorded on the Private Security Services Licence.

5.6.4 All refresher training undertaken by employees shall be recorded and the record held and retained on the employee's personnel file by the employer.

5.6.5 Records shall indicate where further training is required.

6. OPERATIONS

6.1 Risk Assessments

6.1.1 The organisation shall carry out a detailed and documented risk assessment survey on each site documenting the potential risks including security risks, risk to persons on the site, risks to the public and risks to the health and safety of each employee on duty at the site.

6.1.2 The risk assessment shall be in accordance with the risk assessment guidelines contained in **Annex B** to this document.

6.1.3 A Security Management Plan shall be prepared for each site and shall be available to the client and authorised officials. Where applicable, the plan shall include but shall not be limited to the following:

a) the name and contact details (email and mobile phone number) of the representative of the organisation responsible for the implementation of the plan;
b) the risk assessment and risk control plan (always applicable);
c) Numbers of staff and general designation, where defined (always applicable) e.g.
    - Command and Control System team,
    - Supervisors,
    - Enforcement Guards identified by role, for example those responsible for removal of persons, seizure of goods, controlling access and perimeter;
d) Location and time of pre-operation briefing session (always applicable);
e) Crowd management including policy and procedures on searches and removal of persons;
f) Major incident planning;
g) Identification of staff (always applicable);
h) Communications equipment (always applicable);
i) Body Cameras to be worn during the provision of the security service and shall meet all data protection provisions;
j) Traffic management plan as agreed with local Garda Superintendent;
k) Health and safety of staff (always applicable);
l) Personal risk assessment of staff (always applicable);
m) Site plan (always applicable);

n) Details of any subcontractors on site and their role (e.g., locksmiths, alarm technicians etc.);
o) Inclusion of subcontractor's method statement/risk assessment for the specialist tasks they must carry out;
p) Details of any statutory bodies on site and their functions.

6.1.4 All Enforcement Guards shall wear body cameras. The cameras shall be issued to each Enforcement Guard and will only be in use during the periods of operation as set out by the Security Management Plan.

6.1.5 The use of body cameras shall be subject to a Data Protection Impact Assessment (DPIA) and the Data Controller of the organisation is responsible for ensuring that the use of such cameras meet all data protection provisions.

6.1.6 The organisation shall have a Body Camera User Policy in place.

6.1.7 When the body cameras are in use the Enforcement Guard shall indicate to all persons that recording is active and operational via indicator light, switch or slide activation, visible badge, a combination of these indicators or otherwise so that all persons being recorded are aware that the body camera is in record mode.

6.1.8 When the body cameras are not in use, they shall be stored in a safe and secure facility with access restricted to designated officers of the organisation as identified in the DPIA.

6.1.9 All persons required to use body cameras shall have received appropriate and relevant training in the use of the equipment prior to any operation.

.

6.1.10 The number of Enforcement Guards on duty shall depend on the risk assessment and Security Management Plan and shall be determined in consultation with the client.

6.1.11 Notwithstanding the requirements of sub-clause **6.1.10** the organisation shall as a minimum provide the following:
a) at least two Enforcement Guards for each access and egress point to be secured;
b) three Enforcement Guards for each team that is required to remove persons from a site;
c) two Enforcement Guards for each team that is required to remove goods or property.

6.1.12 All Enforcement Guards shall attend a pre-operation briefing session held at a site other than the project site, the content of which shall relate directly to the service being provided, the duration and subject matter of the briefing session depending upon the complexity of the site and operation.

6.1.13 In addition to the pre-operation briefing session each Enforcement Guard and subcontractors shall receive written assignment instructions on what their duties and responsibilities are.

6.1.14 Verification of the pre-operation briefing session shall take the form of an attendance register with the names of attendees in block capitals. The register shall be signed by the attendees including subcontractors, countersigned and dated by the organisation's management.

6.1.15 A copy of the countersigned attendance register shall be attached to the Security Management Plan.

6.2 Times and Hours

6.2.1 Enforcement Guards should be respectful of the religion and culture of others at all times. Consideration should be given to the appropriateness of undertaking enforcement on any day of religious or cultural observance or during any major religious or cultural festival.

6.2.2 Enforcement action in residential settings should only be carried out between the hours of 6.00am and 9.00pm, unless otherwise authorised by a court and in line with relevant legislation. There are no time restrictions on enforcement action in commercial or business premises.

6.3 Mode of entry

6.3.1 Enforcement Guards shall not seek to gain entry to premises under false pretences.

6.3.2 Enforcement Guards shall only enter premises as part of the enforcement process.

6.3.3 Enforcement Guards shall only use a door or other usual means of entry.

6.3.4 The power to enter a premises by force shall only be used when it is reasonably required and only after the Enforcement Manager has authorised the use of said power.

6.4 Goods

6.4.1 Enforcement Guards shall only seize goods or other property in accordance with the terms of the court order.

6.4.2 Enforcement Guards shall ensure that goods are handled with due care whilst in their possession. The organisation shall have insurance in place for goods in transit.

6.4.3 Enforcement Guards shall not remove anything clearly identifiable as an item belonging to, or for the exclusive use of a person under the age of 18 or items clearly identifiable as required for the care and treatment of the disabled, elderly and seriously ill.

6.4.4 A detailed list of all goods removed shall be recorded.

6.5 Vulnerable situations

6.5.1 The organisation and their client have a responsibility to ensure that guidelines are in place on how to proceed where persons have been identified as vulnerable as defined at 2.25 of the definitions in this standard. The use of discretion is essential and the organisation has a duty to contact the client to report the circumstances in situations where there is evidence of possible concern.

6.5.2 The organisation must withdraw from domestic premises if the only person present is, or appears to be, under the age of 18 or is deemed to be vulnerable by the Enforcement Guard.

6.6 Enforcement Manager

6.6.1 The organisation shall appoint a suitably qualified person as Enforcement Manager who shall be responsible for the management of all security services provided by the organisation. The person appointed should hold a managerial position within the organisation.

6.6.2 The Enforcement Manager shall be responsible for ensuring compliance with all PSA legislation, regulations and requirements during the provision of the security service.

6.6.3 The Enforcement Manager shall be on site at all times when a security service is being provided.

6.6.4 The Enforcement Manager shall be in communication with the Command and Control System at all times

6.6.5 All Enforcement Guards shall report to the Enforcement Manager and shall be responsible for all security tasks assigned to them by the Enforcement Manager.

6.6.6 The appointment of a licensed Enforcement Guard to act as an Enforcement Manager is allowable where the Enforcement Manager is not available.

6.7 Command and Control Systems

6.7.1 Facilities shall be in place to provide for the following:

a) The provision, or procurement, of assistance or advice in routine and emergency situations.
b) The recording of all appropriate routine and emergency matters to enable management to deal quickly and efficiently with the organisation's contractual responsibilities.

6.7.2 The organisation shall have a command and control system that is:

a) Located at the organisation’s own fixed location, or
b) A contracted service with a PSA licensed Monitoring Centre.

6.7.3 The following minimum provisions shall apply for all command and control systems.

a) Manning of the operations command and control system shall be consistent with the anticipated workload and the nature of the work.
b) Appropriate first aid and firefighting equipment shall be provided within the command and control system.
c) Management shall review and update command and control system information and procedures at least once every 12 months.

d) Management shall produce a command and control system manual covering all foreseeable contingencies for the guidance of controllers.
e) The manual shall contain instructions for controllers to enable them to deal effectively with all foreseeable contingencies and shall clearly indicate the stage at which any incident requires the controller to pass on information to a more senior person.
f) A copy of the manual shall be readily available within the command and control system at all times.
g) Comprehensive instructions outlining action to be taken on receipt of verbal incident reports shall be provided.
h) There shall be clearly defined procedures for management follow-up in relation to incidents, and also in relation to responses and supports available to staff in the event of an incident.
i) All command and control staff shall be required to partake in practice drills for responses to emergency situations which might endanger the health and safety of staff. Such drills shall take place at least once every 12 months and the outcome(s) of the drills shall be documented and recorded.

6.7.4 The following additional provisions shall apply where the organisation operates its own dedicated fixed location command and control facility:

a) Staff manning the command and control facility shall hold a PSA Enforcement Guard or Security Guard (Guarding) or Security Guard (Monitoring Centre) licence.
b) The equipment, furnishings and layout of the command and control system shall be consistent with the efficient operation of the system.
c) There shall be access to kitchen and bathroom facilities.
d) Heating, lighting and ventilation shall be provided to ensure a reasonable working environment.
e) The command and control system shall be a restricted area open only to those authorised to enter. A means of secure physical restriction shall exist to prevent access by unauthorised persons to the command and control system.

6.7.5 Where a contracted facility is used the organisation shall ensure by initial inspection and documented report that the facility satisfies the requirements of this section and that adequate documented and physical procedures are in place to ensure security of all clients information and access media.

The contract shall include a provision for ongoing periodic inspection and reporting on compliance by the contracted facility to these requirements.

6.7.6 Authorised Officials may access the command and control system for the purpose of verifying compliance with the requirements of PSA licensing.

6.8 Incident Reporting

6.8.1 All operational staff shall be made aware in writing of the identity of the Enforcement Manager and any other member of staff to whom they report and the method of reporting of incidents or problems to the organisation's management, in both urgent and non-urgent cases.

6.8.2 All incidents shall be handled by the Enforcement Manager in the first instance and recorded in the Incident Report. The Incident Report shall contain as a minimum the following details:

a) Date, time and place of the incident.
b) Date and time of reporting and by whom reported.
c) Nature of the incident.
d) Full description of events leading up to the incident, the incident itself and events following the incident.
e) Details and rationale behind the use of any force during the incident
f) Action taken, including onward reporting.
g) Further action to be taken.
h) Where possible, names and addresses of all relevant persons present.

6.8.3 Facilities shall be in place to provide for the following:

a) The recording of all appropriate routine and emergency matters to enable management to deal quickly and efficiently with the organisation's contractual responsibilities.
b) There shall be clearly defined procedures for management follow-up in relation to incidents, and also in relation to responses and supports available to staff in the event of an incident.

6.8.4 There shall be in place an organisation escalation policy for client liaison.

6.8.5 The Organisation shall maintain a record of all reported incidents for a minimum of three years or for such longer periods where required by law.

Entries shall be numbered sequentially and serially and shall include time, date, record of notification of the client and the name of the Enforcement Manager completing the record.

6.9 Threats and Violence

6.9.1 The organisation shall, as part of its risk assessment, assess the risks for violence that employees can reasonably be expected to be exposed to and shall outline and implement risk mitigating measures to eliminate or significantly diminish any identified risks (see **6.1**).

6.9.2 Risk mitigating measures shall include special training and safety routines in place where the risk assessment has shown that there is a significant likelihood and severity of consequence of violence.

Personal Protective Equipment (PPE) shall be provided where it has been identified as a risk mitigation measure.

6.9.3 Safety routines shall be kept continuously updated and shall be made known to all employees, particularly where duties or locations are involved that have been identified in the risk assessment as carrying a higher than normal risk of physical violence occurring. The employer shall ensure that these employees shall be educated, trained and informed in relation to the identified risks.

6.9.4 Tasks involving a high risk of violence shall be identified in the risk assessment and meet the requirements of 6.1.5.

6.9.5 Incidents involving violence shall be recorded and investigated fully by the organisation and notified to An Garda Síochána. Any remedial course of action recommended as a result of the investigation shall be acted upon by the organisation within reasonable timeframes.

6.9.6 The organisation shall ensure that appropriate physical and psychological support is available, on request, to any employee who has been subjected to violence as a result of carrying out his/her duties.

6.10 Operations Records

6.10.1 Records shall be maintained for a period not less than three years for each site, which shall include following information;

a) The service provided and the name of the client(s);
b) Location where the service was provided;
c) Details of the court order including Court reference;
d) Name and PSA Licence Number of the Enforcement Manager;
e) Name, PSA licence number, uniform unique identity number, identification number or works number of each person employed as an Enforcement Guard;
f) Details of all calls made to the command and control system;
g) CCTV/Body Camera footage.

Upon expiration of the required retention period the organisation shall dispose of the relevant records in a secure and confidential manner.

Note: *National legislative requirements may entail retention of records for longer periods of time*.

6.10.2 A facility shall exist for the checking and reviewing of incident reports and reporting procedures periodically by senior management of the organisation. A record of such checks and reviews shall be maintained for a period of 5 years.

6.11 Assignment Instructions

6.11.1 In consultation with the client, the organisation shall formulate assignment instructions, which will encompass full operational instructions for the effective execution of the security service, detailing emergency procedures, lines of communication and accountability.

6.11.2 The assignment instructions shall be agreed and endorsed by the client. Any alteration to the instructions shall be endorsed by the organisation and the client as soon as practicable. Where the client chooses not to endorse assignment instructions the organisation shall maintain evidence on file of e-mailing or postage (registered) of delivery to the client and any subsequent correspondence.

6.11.3 The assignment instructions shall be available in the Security Management Plan and a copy shall be available to the client.

6.11.4 Assignment instructions shall include:

(a) Details of the full extent of the services to be provided;
(b) The procedure for contacting the organisation's command and control system;
(c) Details of the service to be provided including;-
    i. the number of personnel involved in the assignment and their responsibilities,
    ii. the maximum hours allowed for which the service is to be provided shall be 48 hours and handover instructions at start and end of service,
    iii. where security is required after the 48 hour period it shall be provided by a licensee in the Security Guard (Static) sector,
    iv. facilities, vehicles or equipment provided,
    v. safety statement,
    vi. welfare facilities for staff;
(d) A site plan of the location;
(e) Any relevant extracts from the Security Management Plan.

6.11.5 Each Enforcement Guard shall receive individual assignment instructions which shall include the following;

a) Full details of their roles and responsibilities;
b) Name and contact details of their supervisor/manager;
c) Name and contact details of the Enforcement Manager if not included under (b);
d) Location and time of pre-operation briefing session;
e) Start time and duration of operation;
f) Address of site and site plan;
g) Procedures for reporting incidents and responding to incidents;
h) Escalation procedures in the event that the procedure at (g) cannot be activated.

6.12 Security of Information and Access Media

6.12.1 Clear and unambiguous routines shall be established for staff to deal securely with any confidential information to which they have access in the course of operations.

6.12.2 Organisations shall keep confidential any knowledge of their clients' business or operations acquired through the provision of services. In particular, structures and procedures shall be put in place and implemented to ensure that any details relating to the client's security equipment, procedures and practices must be subject to the appropriate level of access within the organisation's business.

6.12.3 Any details relating to the client's business, premises, residence, assets, procedures or any other aspect of knowledge of the client gained by the organisation and employees, the disclosure of which can be reasonably construed as compromising the business or security of the client, shall not be disclosed or made known in any way to a third party or third parties, except with the express written permission of the client.

Where written permission is granted, the organisation shall retain this on file and shall produce this if requested by an appropriate authority.

6.12.4 All confidential information held in electronic format by the organisation shall be backed up at least once a week. Back-up records shall be held in such a manner that a threat or threats to the integrity of one set of records will not pose a threat to the other set.

6.12.5 It shall be a condition of any contract that requires the organisation to hold keys that such keys shall only be surrendered to an authorised representative of the client upon receipt of a written request to do so.

6.12.6 Retention and storage of data relating to CCTV/Body Camera footage taken at the site shall be in line with Data Protection legislation.

All notices, correspondence and documentation issued by the organisation must be clear and in agreement with the client and should comply with relevant legislation.

6.12.7 The organisation should provide a report to the client on any un-executed orders/warrants.

6.13 Vehicles and Equipment

6.13.1 All operational vehicles used by the organisation shall, unless exempted by the risk assessment, clearly display the organisation's name and PSA licence number.

6.13.2 Vehicles shall carry a two-way communication capability, a dry powder fire extinguisher and a first aid kit.

6.13.3 Organisations shall ensure that driving licences of staff involved in driving operational vehicles are valid for the duration of each such employee's period of employment. Copies of all driving licences shall be held on the employee’s file.

6.13.4 Drivers shall complete a history form, to be verified and maintained by the organisation, with all accidents and convictions recorded on this form.

6.13.5 All marked vehicles shall be readily distinguishable from those of any elements of the civil protection or emergency services.

6.13.6 The organisation shall provide all drivers with clearly defined instructions on their role including details of the movement of the vehicle during operations, actions to be taken on foot of incidents, accident procedures, carrying of passengers, etc.

6.13.7 All vehicles and equipment used in connection with the provision of services shall be in working order and be regularly maintained and serviced.

6.13.8 All employees shall sign for all equipment issued and give an undertaking to return any equipment issued immediately on request.

7. COMPLIANCE WITH PSA LICENSING

7.1 Compliance with Standards

7.1.1 Organisations shall maintain compliance with this standard during the term of their licence. Failure to maintain compliance may result in the PSA taking action against the licensee up to and including the revocation of the licence.

7.1.2 Organisations shall be subject to an audit by a PSA appointed auditor at least once during each calendar year or at such intervals as the PSA may prescribe. The purpose of the audit is to verify compliance with the specified standards.

7.1.3 An audit report shall be completed by the auditor for each audit undertaken and the organisation shall agree to the auditor providing a copy of the report to the PSA.

7.1.4 Organisations shall give their permission to the auditor to provide the PSA with information in accordance with provisions **7.1.5** and **7.1.6**

7.1.5 Where an organisation fails to undertake or complete an audit the auditor shall notify the PSA of the failure and the reason for same.

7.1.6 Where an organisation is found to be non-compliant with a standard the auditor shall notify the PSA of the reason for the non-compliance and any resulting action taken against the organisation.

7.2 PSA Licensing Requirements

7.2.1 The organisation shall ensure that an inspector appointed by the PSA may at any time enter any place where a security service is being provided and provide any information requested by an inspector in the course of any inspection or investigation.

7.2.2 Organisations shall be familiar with all legislation relevant to the provision of their business.

7.2.3 During the term of the licence organisations shall comply with all relevant and current legislation and specifically the following:

a) The Private Security Services Acts and Regulations.
b) Organisation of Working Time Acts.

c) Taxation and Social Welfare Acts.
d) Payment of Wages Acts.
e) Immigration Acts.
f) Health and Safety at Work Regulations.
g) Companies Act 2014 (where appropriate).
h) Data Protection Acts.
i) Irish Human Rights and Equality Commission Act 2014.

7.2.4 The organisation shall within 7 days notify the PSA in writing if any of the following occur:

a) Change of name of the licence holder.
b) In the case of a body corporate, change in directors.
c) In the case of a partnership, change in partners.
d) Change of ownership of the organisation. In the case of a body corporate, this includes a change in any shareholding above 5%.
e) Commencement and cessation dates of employment of all enforcement guards.
f) Change of address from which the security service is being provided.
g) Change of registered address if this is different from address at f) above.
h) Change in the legal status of the licence holder.
i) Any conviction against the licence holder whether in relation to the business of the licence holder or other matter. In the case of a body corporate, this includes any convictions against a director. In the case of a partnership, this includes any conviction against a partner.

ANNEX A Screening Forms

Form 1

FORM OF AUTHORITY

I, _____,(BLOCK CAPITALS) hereby

authorise _____

_____

to supply full details of my employment record with the organisation or business in furtherance of my current application for employment in event security.

1. Address at time of employment with the organisation _____

_____

2. PPS No. _____

Signed: _____ Date:_____/_____/_____

Form 2

RECORD OF ORAL ENQUIRY

Name of Applicant: _____

PPS No: _____

Name of Previous Employer: _____

Telephone No: _____

Person Contacted: _____

Dates Employed: - As stated by employee: From _____ To _____

- Confirmed by employer: From _____ To _____

- Would re-employ? _____

- Reasons for not re-employing*: _____

_____

_____

Reasons why applicant would not be suitable to work in security:

_____

_____

_____

Signed: _____ Date: ___/___/___
(Person making enquiry)

Signed: _____ Date: ___/___/___
(Manager)

* Where response indicates that applicant is not suitable for proposed employment bring to immediate attention of Manger responsible for screening/recruitment.

Form 3

REQUEST FOR WRITTEN CONFIRMATION OF INFORMATION PROVIDED ORALLY

RE. Name of Applicant: _____

PPS No: _____

We refer to our conversation with you on the _____ regarding an application for employment in the enforcement guard sector of the security industry made by the above named applicant.

Details of the information which you provided to us orally are enclosed and we would be obliged if you would kindly confirm that these details fairly reflect the information supplied.

Our business is licensed by the Private Security Authority and is obliged by the Authority's regulations to obtain written confirmation of all references we receive in connection with applications for employment.

A copy of a Form of Authority signed by the applicant is enclosed and also a stamped addressed envelope for favour of your reply.

Yours faithfully

_____

Human Resources Manager

Form 4

SCREENING PROGRESS REPORT*

Name of Applicant: _____

PPS No: _____

1. Employments contacted

	Date	Employers Name	Date Letter Sent	Initials	Date of Reply	Initials
1						
2						
3						
4						
5						

2. Screening reviewed

Date of review: __ /__/__ Person Reviewing: _____

Action: _____ Initials: _____

3. Offer of Employment

Signed: _____ Date: ___/___/___
(HR Manager or Principal of the organisation)

4. Employment refused

Signed: _____ Date ___/___/___
(HR Manager or Principal of the organisation)

* This form is to be retained on the individual's file for any subsequent inspection.

ANNEX B Risk Assessment Guidelines

1. Scope

The purpose of these guidelines is to outline the process to be applied by Private Security Authority Licensed Contractors when undertaking Risk Assessments as required by Section 6.1 of the PSA Requirements Document "*PSA Licensing Requirements – Enforcement Guard*".

2. Introduction

Risk assessment and management underlies the duties of PSA Licensed Contractors under the provisions of the PSA Requirements Document "*PSA Licensing Requirements – Enforcement Guard*". Under this document a contractor must identify and assess the risks and select the appropriate control measures to eliminate or reduce those risks so far as is reasonably practicable pertaining to the provision of the security service. A contractor should consider the likelihood, consequences and ways of eliminating or reducing hazards or risks in determining what is reasonably practicable.

This document outlines the processes which should be undertaken along with some of the factors that should be considered by contractors when identifying risks, assessing risks and eliminating or controlling those risks. All elements of the process undertaken in accordance with these guidelines must be documented and available for inspection by the PSA and PSA appointed auditors.

The Requirements Document specifies that a risk assessment shall be undertaken for each site. The extent and level of documentation of risk identification, risk assessment and risk control measures will depend on the circumstances at the time and the likely level of exposure to any risk.

The risk assessment shall be undertaken by a person with competence in security risk identification and in risk assessment and who has the ability to assess all potential risks on a site.

Nothing in these guidelines shall be construed as negating a contractor's **statutory obligations** or requirements under any other enactments or regulations.

3. Security Risk Management (SRM)

The implementation of a Security Risk Management Process (SRMP) will provide a mechanism which ensures that security risks are managed on a systematic basis. This is achieved through the development of a documented and cohesive plan.

The SRMP shall include steps for:

1. the development of a SRM policy which identifies and documents responsibilities and commits to attaining;
    (a) the security of people and property as required by the client,
    (b) a safe and secure working environment.

2. the development of effective security and personnel procedures.

3. employee training and briefing.

4. procedures and controls to be monitored and reviewed.

Within this process contractors shall:

1. identify security risks;

2. assess the risk arising from all security risks identified;

3. prioritise the risks;

4. eliminate or control those risks; and

5. review risk assessments and control measures on a regular basis and immediately after an incident. This also applies to incidents that expose a person in the immediate vicinity to an immediate health or safety risk.

3.1 Identifying Risks

Risk identification relevant to a particular aspect of a contractor's operation (e.g. clients requirements, service provision, site, public interface, recorded incidents, command and control systems, etc) should be considered in the context of service provision as a whole.

Particular consideration shall be given to the location where the service is to be provided (e.g. residential, commercial, agricultural, etc) and the risk associated with such locations.

Attention should also be given to potential risks which could arise as a result of abnormal or

emerging situations (e.g. crowd dynamics, media interest, electrical/technical failures, weather alerts, traffic volumes, etc).

3.1.1 Risk Identification Process

The activities used to identify risks should include but are not limited to the following:

- consulting all relevant historical records relating to incidents;
- consulting client for whom service is being provided;
- consulting employees and/or others who provide the service;
- conducting assessments of site;
- conductions assessments of person(s) present/resident on site;
- conducting assessments of public interface;
- conducting assessments of crowd dynamics;
- conducting assessment of cultural behaviour;
- conducting assessment of access/egress points;
- assessing temporary structures and movable items;
- monitoring adherence to work procedures;
- determining training and skill levels, appropriate to the effective performance of duties;
- assessing the protection of people and property;
- assessing command and control systems;
- assessing vehicles and equipment and
- consulting with customers, An Garda Síochána, Government bodies, representative trade associations and risk assessment consultants on likely security risks.

Potential security risks shall be identified in respect of all aspects of the security service to be provided at the site. These aspects of operations shall include but are not limited to the following:

- the tasks performed;
- the location and surrounds involved;
- procedures;
- the building/structure;
- the assets to be secured;
- persons present including residents, workers, members of the public;
- any resistance to the service taking place;
- the different roles of the staff;
- the roles of sub-contractors;
- the communication methods used;
- the time of day that the work is to be performed;
- use of Personal Protective Equipment (PPE);
- any other equipment or technologies required;
- work practices and procedures, shift working arrangements and other fatigue and stress

related risks;
- manual handling tasks;
- environmental factors (e.g. outdoor, terrain, weather, lighting, traffic and pedestrian flow, intoxication, exposure to blood and other bodily fluids, etc).

3.2 Assessing the Security Risk

After the identification of a risk, the contractor shall assess the risk posed by the risk. This informs the likelihood of an identified risk leading to an incident and the severity of consequence should an incident occur.

3.2.1 Security Risk Assessment

All security risk assessments shall be conducted by a person with appropriate skills and experience in health and safety, security risks and in risk assessment. The assessment shall be conducted in consultation with clients or their nominated representative, employees or other persons involved in the provision of security services.

The risk assessor shall ascertain and take into account (at a minimum) the following factors:

- known risks;
- adequacy of communication systems;
- compliance with regulatory requirements;
- efficacy of PPE for the tasks;
- environmental conditions;
- previous incidents which have occurred;
- site location, structures on site and layout;
- assets being secured;
- persons present;
- any resistance to the service taking place;
- staffing levels required to safely perform the work;
- technical equipment and other hardware;
- type of service required (taking account of public interface and crowd numbers, if applicable).

Factors that shall be taken into consideration when developing systems for the management of risks include but are not limited to:

- the outcome of the security risk assessment;
- information provided by clients and other third parties which may be relevant;
- command and control systems;
- availability of external resources (Gardaí, Fire, Ambulance, Local Authority);
- factors contributing to fatigue and stress (e.g. hours of work, time of day, shift length, number of rest breaks, amount of time between breaks, potential or actual exposure to

workplace violence);

- the level of skill and experience of the staff carrying out the work;
- backup services including availability of additional staff and resources.

3.2.2 Establishing the Priority of Risks

Once the risks have been assessed the next step is to prioritise them for remedial action. All risks shall be dealt with in an appropriate manner and as soon as possible. While a high level of risk is the priority for corrective action, any medium or low level risk should not be ignored.

Contractors will be required to follow a four stage approach in prioritising risks:

Stage 1. Determine the likelihood of a risk related incident occurring.

Stage 2. Should an incident occur, determine its consequences and severity.

Stage 3. Combine the results of stages 1 and 2, to rate the level of the risk. The Risk Assessment Matrix set out at page 9 provides a template of how this should be recorded.

Stage 4. Prioritise the risks according to the outcomes of stage 3. This priority will be used in compiling and implementing a risk control plan.

3.3 Eliminating, Diminishing and Managing Risk

The risks identified and the assessment of the level of risk will determine the steps taken to manage those risks. The goal of the steps taken should be to eliminate or sufficiently manage the risk. These steps should not result in the creation of additional risks. Notwithstanding the obligation of contractors to comply with the PSA Requirements Document, consideration should be given to the following when setting risk mitigating and control measures in a risk control plan.

3.3.1 Elimination of Risk

The primary measure which should always be considered is the elimination of the risk. Notwithstanding the desirability of introducing a measure which completely eliminates the risk, one of the following risk management or control processes shall be undertaken where elimination of the risk is not possible.

3.3.2 Substitution of Risk

Replace the risk with one which carries a lower level of risk.

3.3.3 Risk Isolation

Isolate the risk, and in so doing prevent exposure to the risk.

3.3.4 Minimizing Exposure to Risk

The exposure to the risk may be reduced through:

- Engineering means or
- Administrative means or
- The appropriate use of PPE.

Examples of measures which may be used to manage risk include but are not limited to:

- Staffing levels;
- Equipment or technologies used for the protection of personnel and valuables;
- Implementation, development and adherence to secure work practices;
- Communication methods;
- Supervision;
- Training; and
- Command and Control systems.

3.4 Monitoring and Reviewing the Plan

Management of risks is an ongoing, evolving process. It is a cornerstone of business management and as such should be checked and reviewed periodically and as circumstances dictate. The process of identification, assessment and determination of control measures should be repeated when risk assessments and risk management measures are being reviewed. All those who are potentially affected by the change shall be consulted during the risk management process and informed of new requirements at completion.

4. Risk Assessment Template

The template on page 50 provides a basic format for all risk assessments referred to and required within the Requirements Document. A contractor may substitute another format for the risk assessment provided it has, as a minimum, the headings provided in the template. The template will assist contractors to:

- identify the risks,
- assess the level of risks,
- prioritise the risks and
- control and manage the risks.

A table shall be completed for each task and element of the security service being provided and should contain a comprehensive list of all identified risks and consequent assessed risks associated with each of those tasks and elements within the service provision. Please note that the five rows shown here are for illustrative purposes only and more may be added as appropriate.

Security Risk Assessment Methodology

Section 1: Context

1.1 Site Details

Client Name			
Site name			
Site location			
Name of assessor		Date of assessment	
Status (Draft/Final)			

1.2 Scope

An overview of the purpose of the report.

1.3 Purpose

Details as to why the report is required, it's aspirations or desired outcomes, who contributes and who sees the final document

1.4 Methodology

Details on how information relied upon for the report was gathered, this is completed last when the methodology is clear

1.5 Available Information

A well detailed section documenting all information currently available, including commentary on the premises location, the physical environment and structure, persons known to be on the premises, etc..

Section 2: Risks and Solutions

2.1 Risk Identification

Details of all risks including the origin of the risk and the consequences of events if the hazard/risk where to materialize. Risks should be placed in order of priority.(This section can be expanded as required)

Priority	Risk Identified	Severity	Consequences

2.2 Controls

Details of recommendations/countermeasures proposed and reasons why, with comments on feasibility or restrictions/impediments. (This section can be expanded as required)

Priority	Risk Identified	Control	Reasoning

Section 3: Risk Analysis and Evaluation

LVI Table Matrix

Rating	Likelihood	Vulnerability	Impact
1	**Extremely Improbable**- A incident could only occur in extreme circumstances.	**Very low** – The business has more than adequate risk controls currently in place with redundancy and training in place.	**Negligible** - Slight or no disruption to business operation. No risk of harm.
2	**Improbable** – An incident may occur if other factors were present, but the risk is minimal.	**Low** - The business has more than adequate controls currently in place but without redundancy or training in place.	**Slight** - Minor delay to operations, minor asset damage, emotional impact to staff.
3	**Possible** – An incident may occur in conjunction with other factors.	**Medium** - The business has some risk controls in place however they are not adequate and require supporting measures.	**Moderate** – Operations delayed or disrupted. Moderate asset damage. Physical harm or psychological harm to staff.
4	**Probable**- An incident will most likely occur in the absence of further controls.	**High** – The business has minor risk controls in place however there are serious deficiencies in the adequacy of this controls.	**Serious** - Operational failure. Serious asset damage. Serious injury to staff.
5	**Highly Probable** – An incident will certainly occur in the absence of further controls.	**Very High** - There are no risk controls in this area or serious aggravating risk factors in place.	**Very Serious** – Operational failure, critical asset damage, death or serious injury to staff.

Risk Rating

Category	Score	Description
Critical	65 -125	Immediate action essential to address a specific security vulnerability
High	36 - 65	Immediate action recommended for effective security provision
Medium	11 - 35	Action recommended for a comprehensive security provision
Low	0-10	Currently controlled

Risk Assessment Template

Asset/Activity	Threat	Risk Description	L	V	I	R	Recommended Controls	L	V	I	R

KEY to TEMPLATE:

L = Likelihood of risk occurring (rating is within the range of 1 to 5 with 1 being the least likely to occur and 5 being the most likely to occur) V = Potential Vulnerability (rating is within the range of 1 to 5 with 1 being the least vulnerable and 5 being the most vulnerable)

I = Impact (rating is within the range of 1 to 5 with 1 being the least impact and 5 being the greatest impact)

R = (this is arrived at by multiplying the numerical values assigned to likelihood, vulnerability and impact respectively as above). L x V x I = R on a scale of 1 to 125 with 125 being the highest risk.

ANNEX C Cash Flow Template

Cash Flow Statement From							To					
Cash In	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
Sales												
Own Funds												
Loans												
Overdraft												
Other Incomings												
Total Cash In												
Cash Out	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
Sales Costs												
Rent												
Insurance Costs												
Wages												
Equipment Costs												
Uniform Costs												
Overheads												
Loan Repayments												
Tax • Employer PAYE / PRSI • Income / Corporation Tax • VAT												
Other Outgoings												
Total Cash Out												
Cash Flow: Surplus/(Deficit)												
Opening Cash Balance												
Closing Cash Balance												