



An tÚdarás Slándála Príobháidí  
The Private Security Authority

*The Security Regulator*

# Public Consultation

Requirements for Access Control Contractors in the Private Security Industry.

<b>Summary of Public Consultation</b>	
<b>Agency:</b>  Private Security Authority	<b>Legislation:</b>  The Private Security Services Act 2004 and 2011
<b>Subject:</b> Electronic Security - Access Control	<b>Date:</b> 29 <sup>th</sup> May 2017
<b>Related publications:</b>  None	
<b>Contacts for enquiries:</b> Siobhan Carew: 062-32615 Josephine Crowe: 062-32616	<b>Email:</b>  <a href="mailto:public_consultation@psa.gov.ie">public_consultation@psa.gov.ie</a>

## Agency and Legislation

The Private Security Services Act 2004, as amended, established the Private Security Authority (PSA) as the statutory body with responsibility for the licensing and regulation of the security industry in Ireland. The functions of the PSA as set out in section 8 of the Act include, the specification of qualifications or any other requirements (including requirements as to training) for the grant of licences.

Section 2 of the Private Security Services Act sets out the categories of security service to be licensed by the PSA. The PSA licences both contractors and individuals. This public consultation relates to the licensing of contractors only.

### Why is this Public Consultation being issued?

The PSA currently licence contractors in the Electronic Security - Access Control sector. Contractors in the sector are required to comply with the standard, SR40, in order to obtain a licence. One of the key strategic goals of the PSA is to raise standards within the industry. In pursuit of this goal, the PSA wishes to prescribe new requirements which contractors must meet and adhere to.

The PSA is concerned that the level of service currently being provided in this area is not being delivered in a consistent and safe manner across all providers. The security industry and the public expect all those working in the industry to provide an effective security service without posing any undue risk to the public. The PSA believes that the Requirements Document set out in this consultation will contribute to meeting this expectation.

## **PSA Requirements for Installers of Access Control**

The PSA has produced a draft document which sets out the requirements which shall apply to contractors who install, maintain, or service access control systems including automatic gates. The document is titled “*Standard For The Licensing Of Access Control Contractors (PSA67:2017)*” and is attached.

### **Responding to this Public Consultation**

This Public Consultation is being issued for the information of contractors, industry stakeholders, interested parties and the public. Comments on same should be made to the PSA by the 10<sup>th</sup> July, 2017.

By email at: [public\\_consultation@psa.gov.ie](mailto:public_consultation@psa.gov.ie)

or

By post to:                   The Private Security Authority  
                                  Davis Street  
                                  Tipperary Town  
                                  Co Tipperary  
                                  E34 PY91

The closing date for receipt of comments is Monday 10<sup>th</sup> July, 2017.



An tÚdarás Slándála Príobháidí  
The Private Security Authority

*The Security Regulator*

## **PUBLIC CONSULTATION DOCUMENT**

# **PSA LICENSING REQUIREMENTS**

## **Electronic Security - Access Control**

### **(PSA 67:2017)**

Standard For The Licensing Of  
Access Control Contractors

May 2017  
[www.psa.gov.ie](http://www.psa.gov.ie)

## Contents

<b>1.</b>	<b>SCOPE</b>	<b>6</b>	
<b>2.</b>	<b>DEFINITIONS</b>	<b>7</b>	
<b>3.</b>	<b>ORGANISATION</b>	<b>9</b>	
	3.1	Ownership	9
	3.2	Finances	10
	3.3	Insurance	10
	3.4	Premises	10
	3.5	Organisation Information	11
	3.6	Quotations in pursuance of Contracts or Business	11
	3.7	Compliance with Legislation	12
<b>4.</b>	<b>STAFFING</b>	<b>13</b>	
	4.1	Selection and Pre Employment Screening	13
	4.2	Terms of Employment	17
	4.3	Code of Conduct	17
	4.4	Identification	18
<b>5.</b>	<b>TRAINING</b>	<b>19</b>	
	5.1	Training Policy and Responsibility	19
	5.2	Induction Training	19
	5.3	Specialist Training	199
	5.4	Refresher Training	19
	5.5	Supervisory and Management Training	19
	5.6	Training Records	20
<b>6.</b>	<b>OPERATIONS</b>	<b>21</b>	
	6.1	Planning and Design	21
	6.2	Installation	22
	6.3	Test and Commission	22
	6.4	Maintenance, Service and Repairs	23
	6.5	Call Outs	24
	6.6	Legislation	24
	6.7	Security	24
	6.8	Vehicles and Equipment	25
<b>7.</b>	<b>POWERED GATES</b>	<b>26</b>	
	7.1	Powered Gates	26
<b>8.</b>	<b>COMPLIANCE WITH PSA LICENSING</b>	<b>28</b>	
	8.1	Compliance With Standards	28
	8.2	PSA Licensing Requirements	28
	<b>ANNEX A</b>	<b>30</b>	
	<b>ANNEX B</b>	<b>34</b>	

## 1. SCOPE

This standard provides a specification for compliance with licensing by the Private Security Authority and applies to contractors seeking licences to provide security services as Access Control contractors.

The Government of Ireland through the Private Security Services Act, 2004, 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 Private Security Authority and those seeking a licence from the PSA must comply with this standard. Only certification bodies approved by the PSA may provide certification services for licensing purposes. Contractors should check the PSA website, [www.psa.gov.ie](http://www.psa.gov.ie), for a list of approved certification bodies.

By applying for and holding a licence, contractors agree to the sharing of information relating to this document, the contents herein and any audit (including audit reports) undertaken for the purposes of PSA licensing between the PSA and the contractor's certification body. Where a contractor fails to comply with the requirements of this standard, the certification body is obliged to notify the PSA.

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](http://www.psa.gov.ie).

## 2. DEFINITIONS

- 2.1 Access Control.** The control or recording of access by persons or vehicles to or within premises by means of:
- a) Personal identity verification, including by means of biometrics
  - b) Vehicle identification
  - c) Numerical codes
  - d) Alphabetical codes
  - e) Access or other card management,
  - f) Electronic key management, or
- or any combination of such means.
- 2.2 Ancillary Staff.** All security organisation staff not directly employed in duties falling within the definition of occupations covered by this standard who may have access to information of a confidential nature.
- 2.3 Approved Certification Body.** A certification body approved by the PSA to provide certification services in respect of Access Control.
- 2.4 Assessment.** Test carried out to certify the competence of all officers.
- 2.5 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.
- 2.6 Basic Training.** Qualification required by all employees to meet the mandatory training requirements in respect of PSA licensing.
- 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 and signed 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 Identity Badge.** The identification card or licence card held by the employee to be visibly worn by operational security staff whilst on duty, the design and conditions of which are as specified from time to time by the PSA.
- 2.10 Induction (Training).** The organisation-specific induction briefing session covering organisation structure, ethos, policies and including the organisation's and employee's roles and responsibilities.
- 2.11 Licence Card.** The official identification card issued by the PSA to each individual employee licence holder to verify his or her licence status.

- 2.12 Organisation.** A limited or unlimited company, a partnership or sole trader providing services installing, maintaining, repairing or servicing security equipment that consists of electronic or other devices designed, constructed or adapted to control or record access by persons or vehicles to or within premises where such equipment is situated, for which a PSA installer of security equipment (Access Control) licence is required.
- 2.13 Powered Gate.** An access control system, which electronically controls gates giving access to or within a premises.
- 2.14 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.
- 2.15 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.
- 2.16 Private Security Authority (PSA).** The regulatory and licensing authority for the private security industry in the Republic of Ireland.
- 2.17 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.
- 2.18 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.
- 2.19 Screening Period.** Period of not less than five years prior to the date of the application for relevant employment or transfer to relevant employment.
- 2.20 Security Service.** The provision of access control services for which a PSA licence is required.
- 2.21 Site:** The premises, property, area or complex at which the service is carried out.
- 2.22 Training Administrator.** A person within the organisation appointed to supervise and record all aspects of training within the organisation.
- 2.23 Verification.** Confirmation by sight and written records held at the organisation's premises.



## **3. ORGANISATION**

### **3.1 Ownership**

- 3.1.1** Except in the case of a plc, ownership and management of the service provider shall be clearly stated in writing, and all individuals having ownership, shareholdings or control of more than 5% and the company secretary shall be properly identified.
- 3.1.2** The names of all directors of the organisation shall be established and recorded and a record of the results of the screening of such directors to be held on file and disclosed to an authorised person on request.
- 3.1.3** 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 field of access control within the previous 10 years,
  - b) Qualification as an electronic security services apprentice or equivalent,
  - c) such other means as may be approved by the PSA.

*Note: Where an organisation is a limited or unlimited company, at least one director must demonstrate that they possess the required competence, where an organisation is a partnership at least one partner must demonstrate that they possess the required competence, all sole traders must demonstrate that they possess the required competence.*

- 3.1.4** Where directors involved in operational activities are also employees of the organisation they shall hold a current PSA employee licence covering, as a minimum, the primary service provided by the organisation.
- 3.1.5** Details of discharged or undischarged bankruptcy of a principal or director of the organisation shall be held on file and disclosed to the client on request.
- 3.1.6** Where applicable, all principals of the organisation shall sign a declaration setting out their beneficial interests in other organisations subject to licensing by the PSA.
- 3.1.7** All operational supervisory and management staff shall hold a current PSA employee licence in accordance with PSA requirements, for each activity subject to the PSA licensing, carried out by such staff.

## **3.2 Finances**

**3.2.1** The organisation shall ensure compliance with Tax Clearance during the term of the licence. Holders of eTax Clearance certificates shall provide the TRN and 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 on request by authorised officials a projected cash flow statement for the next 12 months. For new organisations, a cash flow forecast for the first 12 months of business shall be provided. (see Annex B for suggested format)

## **3.3 Insurance**

**3.3.1** All insurances shall be 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
- Product Liability
- Motor insurance
- Professional indemnity

## **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 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.

## **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** Where the provision of a contract is required by a client such contract 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 (installation/maintenance) 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) Details of complaints procedures and complaints management procedures
  - f) 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** Where the use of subcontractors is provided for under the terms of the contract or agreement, the organisation which is the party contracted to provide the service to the client shall require the subcontractor to provide evidence of compliance with prescribed standard(s), as well as evidence of holding a current valid PSA licence, before engaging the services of that subcontractor.

## **3.6 Quotations in pursuance of Contracts or Business**

- 3.6.1** Each organisation 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.
- 3.6.3** The provisions of **3.6.1** and **3.6.2** do not apply in the case of emergency call outs. However, in all cases not covered by **3.6.1** and **3.6.2** the prospective client shall be provided with a verbal quotation in advance of all work.

### **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.
- National and EU product compliance legislation.

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

- The Private Security Authority.
- Certification bodies approved by the Private Security Authority.

## **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 Probationary employment should be for a period of 6 months and in no case shall exceed a period of nine months.
- 4.1.1.6 Certified copies of all relevant personnel and screening documentation shall be held on file.
- 4.1.1.7 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.
- 4.1.1.8 The relevant provisions of these requirements shall apply to all ancillary staff including those employed on a temporary basis.
- 4.1.1.9 The screening period shall not be less than five years or from school leaving, whichever is the shorter duration.
- 4.1.1.10 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.
- 4.1.1.11 Screening covering the whole of the screening period shall be completed no later than ten weeks after employment has commenced.

4.1.1.12 Full screening for the period covered under **4.1.1.9** 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.

4.1.1.13 Where the provisions of **4.1.1.12** 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.
- 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 for written confirmation of the information given by telephone shall be forwarded to the referee within two working days of the telephone call being made (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 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 Office of the Data Protection Commissioner.
- 4.1.6.3 A list of all personnel currently employed both on a permanent and a probationary basis shall be maintained, and in the case of those employed on a probationary basis, giving the dates on which probationary employment commenced and is to cease for each individual.



## **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 clients premises.
- h) Ensure that they use employer's equipment or facilities only with authorisation.
- i) Continuously satisfy the requirements of PSA licensing.
- j) Wear a correct identity badge or licence card, as prescribed by the PSA, 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 Identification**

**4.4.1** The organisation shall ensure that all employees have an identity badge either in the form of an organisation issued badge, satisfying criteria prescribed by the PSA or alternatively the PSA issued licence card.

**4.4.2** All employees shall be instructed on PSA requirements for wearing an identity badge.

**4.4.3** Where the organisation provides its own identity badge, it shall ensure its periodic review. The duration between periodic reviews cannot exceed 24 months.

**4.4.4** There shall be in place formal arrangements for the withdrawal of organisation issued identity badges from an employee on request.

CONSULTATION

## **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 Private Security Authority.
- 5.1.2 The organisation shall appoint a member of the management team as training administrator.
- 5.1.3 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. 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 involved in the design, installation, maintenance, repair and servicing of systems have the necessary training to undertake such tasks competently and safely.
- 5.3.2 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.
- 5.3.3 Where risks are identified, in the course of carrying out a risk assessment under 6.1, 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 on site 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.

CONSULTATION

## **6. OPERATIONS**

All access control systems must comply with the following European Standards;

- a) EN 60839-11-1:2013
- b) EN 60839-11-2:2015

and the operational requirements set out in Section 6. Where there is a conflict between the requirements of the European Standards and the requirements of Section 6, the requirements of this document shall take precedent unless otherwise provided for by the PSA.

Contractors who install, maintain, repair or service powered gates must also comply with Section 7 of this requirements documents.

### **6.1 Planning and Design**

**6.1.1** The organisation shall on the first visit to the site where the service is to be provided assess the clients requirements against any agreed contracted service, the security risk and the physical environment.

**6.1.2** As part of the site visit at **6.1.1** the organisation shall identify each access point and shall evaluate each access point under the following:

- physical environment (walls, fences, slopes, etc)
- location of access points (indoor/outdoor, environment, etc)
- level of security required,
- user levels (flow of persons/vehicles at peak and non peak times),
- access levels for users,
- integration with other systems (intruder alarm, CCTV, Fire etc),
- safety requirements (emergency exits, fire protection, type of user (children, disabled), safety of users and public, electrical, etc),
- protection of system from weather, vandalism, accidental damage,
- manufacturers requirements,
- cabling (cable routes, cable types, etc),
- backup systems (power supply, equipment failure, releases, etc),
- management system,
- building regulations.

**6.1.3** A risk assessment shall form part of the site visit at **6.1.1**.

**6.1.4** Where the risk assessment identifies a weakness or residual risk in any agreed contracted service, this shall be advised to the client and a decision sought on how to proceed. A record of this decision, detailing measures to be undertaken shall be recorded before any work commences and the client advised of any revised costs. In order to minimise risks, visual warnings shall be utilised to reduce the likelihood of an incident.

**6.1.5** A System Design Proposal, which shall take into account the findings of the site visit and risk assessment, shall be prepared and agreed with the client.

**6.1.6** The System Design Proposal shall include a site plan which shall detail the physical environment and the location of each access point.

## **6.2 Installation**

**6.2.1** The system shall be installed in accordance with the System Design Proposal by installers with the necessary training and experience.

**6.2.2** Any alterations to the System Design Proposal shall be agreed with the client and the document shall be amended accordingly.

**6.2.3** All electrical work shall comply with current national legislation and carried out by persons qualified to do so.

**6.2.4** The installation shall be carried out in accordance with the manufacturer's policy and instructions and meet manufacturer's specifications.

**6.2.5** All systems, and their installation shall comply with the European Machinery Directive (2006/42/EC) including health and safety requirements.

## **6.3 Test and Commission**

**6.3.1** On completion the system shall be inspected to confirm that it has been installed in accordance with the System Design Proposal. Any deviations shall be included in the As Fitted Document.

**6.3.2** The system shall be tested, and the results compared against the requirements included in the System Design Proposal as amended by the As Fitted Document. A record of tests carried out shall be recorded in the safety file.

**6.3.3** The organisation shall provide the client with training on the operation and maintenance of the system.

**6.3.4** Clients shall be informed of any codes or passwords required to access the system and on the method of changing such codes and passwords. Clients shall be advised to change codes and passwords and not to retain default settings.

**6.3.5** Clients shall be advised of the procedure to enable release in an emergency.

**6.3.6** On completion of the installation the client shall receive the following documentation:

- a copy of the System Design Proposal as amended by the As Fitted Document,
- user manual,
- EU declaration of conformity,
- service and maintenance instructions,
- safety file,
- log book to include the following details
  - name, contact details and PSA licence number of installer,
  - manufacturers product name of system and manufacturers details,
  - date of commissioning,
  - space to record all details of maintenance, servicing, repairs, alterations including the name of the organisation undertaking such work, their employees name and the date(s) the work was undertaken.
  - Space to record next date for scheduled maintenance.

## **6.4 Maintenance, Service and Repairs**

**6.4.1** It is the client's responsibility to arrange for the installation to be properly maintained (inspected and serviced) and repaired as scheduled or necessary.

A documented arrangement should be made between the client and the organisation for the repair and maintenance of the installation. The arrangements shall specify the schedule of maintenance agreed including:

- a) the frequency of maintenance required,
- b) the requirements of such maintenance.

**6.4.2** The client shall be informed in advance of the date on which the maintenance shall be carried out and the identity of the person who shall carry out the maintenance.

**6.4.3** Where an organisation visits a site for the first time it shall undertake a site visit and risk assessment in accordance with the requirements of section **6.1** and request the log book, and safety file for the system from the client.

**6.4.4** All procedures used in the maintenance, servicing and repair of access control and powered gates shall be in accordance with manufacturer's policy and instruction and meet manufacturers specifications.

**6.4.5** Any repairs or alterations to the system necessary following maintenance are to be performed in such a way as to return the system to the same level of service or better, as provided before the maintenance. Alterations shall be in accordance with the manufacturers technical document. Where this is not possible, the client is to be advised and direction sought.

**6.4.6** Any component replaced shall be of the same or increased level of security as the original component and shall not impact on the functionality or safety of the system. Where the client requests a component of a lower level of security this request shall be made in writing. Such a request shall be retained on the file of the organisation.

**6.4.7** Following repairs, alterations or replacement of any major component, testing shall be carried out in accordance with the requirements of section **6.3**, the CE marking updated and the safety file updated.

## **6.5 Call Outs**

**6.5.1** Organisations shall provide a 24 hour call out service with emergency attendance within 3 hours of receipt of a call out.

**6.5.2** Where an organisation is called out to access a premises they shall satisfy themselves as to the identity of the client and their entitlement to request access to the premises before undertaking any work. A driving licence, passport or other photo id should be requested together with documentary proof that they are entitled to access the premises (utility bill in clients name, permission to request service on company letterhead or similar).

**6.5.3** Where an organisation is not satisfied as to the identity of the client or their entitlement to request access, the organisation should request that An Garda Síochána be notified that access has been requested. Evidence that the request to An Garda Síochána has taken place should be provided to the organisation. If the client refuses to notify An Garda Síochána, no work should take place and the organisation should notify An Garda Síochána of the incident.

**6.5.4** Where a call out takes place the Record of Call Out Form at Annex B shall be completed and signed by the client and organisation.

## **6.6 Legislation**

**6.6.1** All installations, maintenance, repairs and servicing shall be conducted in accordance with health and safety, building, electrical and fire regulations.

**6.6.2** All installations, maintenance repairs and servicing of equipment connected with escape routes shall be conducted in accordance with EN179, EN1125 and such other requirements as prescribed by law.

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

## **6.7 Security**

**6.7.1** Procedures shall be established for all staff to ensure the security of information and property to which they have access during the course of their employment.

**6.7.2** 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 company or business.



- 6.7.3** 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.
- 6.7.4** It shall be a condition of any contract that requires the organisation to hold keys/codes that such keys/codes shall only be surrendered to an authorised representative of the client upon receipt of a written request. Where the client does not give written authorisation the organisation shall not surrender the keys referred to above. The organisation shall comply with any PSA licensing requirement for key holding.
- 6.7.5** Organisations shall have procedures in place to ensure the security of information held in an electronic format. Appropriate security measures such as passwords and encryption shall be in place and back up records held securely. Confidential records held in an electronic format shall be backed up at least once a week. Back up records shall be held securely and in such a manner that a threat to the integrity of one set of records will not pose a threat to the other set.
- 6.7.6** It shall be a condition of any contract that requires the organisation to have access to the client's terminals or servers either on-site or off-site, that the organisation take appropriate security measure to prevent unauthorised or unlawful access to the terminals and/or servers.
- 6.7.7** A record of visits to all client premises shall be kept for a minimum of three years and shall include details of the service provided and the name and PSA licence number or works number of the person(s) who provided the service. 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.

## **6.8 Vehicles and Equipment**

- 6.8.1** All liveried vehicles shall clearly display the organisation's name, badge or logo and telephone number(s).
- 6.8.2** Employers 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. Driving licences shall be inspected annually and a record of this kept on file.
- 6.8.3** All vehicles and equipment used in connection with the provision of services shall be in working order and be regularly maintained.
- 6.8.4** All employees shall sign for all equipment issued and give an undertaking to return any equipment issued immediately on request.

## 7. POWERED GATES

This section sets out additional requirements to be followed by contractors who install, maintain, repair or service powered gates. Such contractors shall also comply with the following European Standards;

- a) EN 12453:2000
- b) EN 12635:2001 + A1 2008
- c) EN 12978:2003 + A1 2009
- d) EN 13241-1:2003 + A1 2011

Where there is a conflict between the requirements of the European Standards and the requirements of Sections 6 or 7, the requirements of this document shall take precedent unless otherwise provided for by the PSA.

### 7.1 Powered Gates

7.1.1 The System Design Proposal under 6.1 shall consider the following hazards;

- Any points where persons may be injured by being crushed or trapped, for example:
  - meeting point between swing gates when closing,
  - sliding gates at end of travel position,
  - trapping of feet between lower edge of gate and ground,
  - space between a moving gate and a fixed object,
  - contact with moving parts at the drive unit;
- hazards from being caught or hooked by sharp edges or projections;—
- the impact forces produced by a gate when it strikes a person or an obstacle;
- hazards associated with the gates being activated automatically, or by another person (for example, by a sensor under the road surface activating a gate when a car drives over it, a remote button, a key fob pressed by a third party or a gate operated by dialling a mobile phone);—
- possible ways in which safe operating systems (such as key-pad or key-fob systems) could be defeated, bypassed or inappropriately operated, thereby placing any person at risk. (This is particularly relevant where children, members of the public, or persons not familiar with a location have access to powered gates and may not recognise a risk to their safety);
- the possibility of gates becoming detached from their supports and falling over;
- all danger zones up to a height of 2.5m should be identified; and
- electrical hazards, such as electric shock or erratic behaviour due to ingress of moisture on electrical circuits.
- risks arising from the following factors;
  - use by children,
  - use by infirm or elderly people,
  - unrestricted access or other instances when it is not possible to instruct, train or supervise the gate users,
  - high frequency of use or large number of people passing by, or
  - a high degree of automation.

- 7.1.2** All gates shall have an isolator switch which shall be clearly visible and located next to the gates.
- 7.1.3** As part of the documentation provided under clause 6.3.6, clients shall be advised that preventative maintenance should take place on an annual basis.
- 7.1.4** Where a gate is found to be unsafe the client shall be informed and advised of any remedial work required. The organisation and the client shall agree a programme of remedial work and the cost.
- 7.1.5** Gates shall not be left in an unsafe condition.

CONSULTATION

## **8. COMPLIANCE WITH PSA LICENSING**

### **8.1 Compliance With Standards**

- 8.1.1** Organisations shall maintain compliance with this standard during the term of the licence. Failure to maintain compliance may result in the PSA taking action against the licensee up to and including the revocation of the licence.
- 8.1.2** Organisations shall be subject to an audit by an approved certification body 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.
- 8.1.3** An audit report shall be completed by the approved certification body for each audit undertaken and the organisation shall agree to the certification body providing a copy of the report to the PSA.
- 8.1.4** Organisations shall give their permission to the approved certification body to provide the PSA with information in accordance with provisions **8.1.5** and **8.1.6**
- 8.1.5** Where an organisation fails to undertake or complete an audit the certification body shall notify the PSA of the failure and the reason for same.
- 8.1.6** Where an organisation is found to be noncompliant with a standard the certification body shall notify the PSA of the reason for the non compliance and any resulting action taken against the organisation.

### **8.2 PSA Licensing Requirements**

- 8.2.1** 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.
- 8.2.2** During the term of the licence organisations shall comply with all relevant and current legislation and specifically the following:
- a) The Private 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) European Product Legislation.
  - h) Building Regulations
- 8.2.3** 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 company directors.
  - c) In the case of a partnership, change in partners.
  - d) Change of ownership of the company. In the case of a body corporate this includes a change in any shareholding above 5%.

- e) Change of address from which the security service is being provided.
- f) Change of registered address if this is different from address at d) above.
- g) Change in the legal status of the licence holder.
- h) 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 company director. In the case of a partnership this includes any conviction against a partner.

CONSULTATION

# ANNEX A

## Screening Forms

*Form 1*

### FORM OF AUTHORITY

I, \_\_\_\_\_, (BLOCK CAPITALS) hereby authorise

\_\_\_\_\_  
\_\_\_\_\_

to supply full details of my employment record with the company or business in furtherance of my current application for employment in the security industry

1. Address at time of employment with the company \_\_\_\_\_

\_\_\_\_\_

2. PPS No. \_\_\_\_\_

Signed: \_\_\_\_\_ Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

**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 the access control sector:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Signed: \_\_\_\_\_

(Person making enquiry)

Date: \_\_\_/\_\_\_/\_\_\_

Signed: \_\_\_\_\_

(Manager)

Date: \_\_\_/\_\_\_/\_\_\_

\* Where response indicates that applicant is not suitable for proposed employment bring to immediate attention of Manager 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 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



**SCREENING PROGRESS REPORT\***

Name of Applicant: \_\_\_\_\_

PPS No: \_\_\_\_\_

1. Employments contacted

	<b>Date</b>	<b>Employers Name</b>	<b>Date Letter Sent</b>	<b>Initials</b>	<b>Date of Reply</b>	<b>Initials</b>
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 company)

4. Employment refused

Signed: \_\_\_\_\_ Date \_\_\_/\_\_\_/\_\_\_  
 (HR Manager or Principal of the company)

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

# ANNEX B

## RECORD OF CALL OUT

Name of Client: \_\_\_\_\_

Address of Client: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Clients Phone No.: \_\_\_\_\_

Name of Person Requesting Access \_\_\_\_\_  
(if different from client)

Details of Access Requested: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Time and Date of Request: \_\_\_\_\_

ID Verified: YES/NO      Type of ID: \_\_\_\_\_

Entitled to make Request: YES/NO.      Means of Verifying Entitlement: \_\_\_\_\_

Time and Date of Call Out: \_\_\_\_\_

Details of Call Out: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

The client/requesting party declares to have all the legal rights, powers and faculties to request the callout service and takes full legal responsibility for any consequences deriving from the callout. The client/requesting party also takes full responsibility of the contractual obligations with the organisation carrying out the callout service and agrees to fully cover the callout charges where the service cannot be undertaken due to unforeseen circumstances.

Clients/Requesting Party's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Organisations Representative Signature: \_\_\_\_\_ Date: \_\_\_\_\_

CONSULTATION