



An tÚdarás Slándála Príobháidí
The Private Security Authority

A STANDARD FOR PSA LICENSING

PUBLIC CONSULTATION DOCUMENT

FUTURE REQUIREMENTS FOR THE LICENSING OF EVENT SECURITY CONTRACTORS

November 2013

PUBLIC CONSULTATION

The Private Security Authority (PSA) is seeking submissions on “*A Standard For PSA Licensing – Future requirements for the licensing of Event Security Contractors*”. This public consultation process offers the security industry and other interested parties an opportunity to engage in the development of the standard.

The document is part of the development process for the licensing of *Event Security* contractors. Our aim is to develop a standard which will support the licensing regime and will be relevant to the environment in which *Event Security* contractors operate. The PSA will announce a timeframe for the licensing of *Event Security* contractors when this public consultation concludes.

This document relates to the licensing of contractors only. The licensing of individuals (employees) will take place at some future stage and will be the subject of a separate development process. A timeframe for the licensing of individuals has not yet been set out.

In developing this document the PSA has considered the following codes of practice;

- Safety at Outdoor Pop Concerts and other outdoor musical events,
- Safety at Sports Grounds,
- Safety at Indoor Concerts,

and has adopted some of the clauses therein to this document.

“*A Standard For PSA Licensing*” is a discussion paper which sets out what the licensing requirements for *Event Security* contractors might be. The PSA are inviting submissions and comments from the security industry and other interested parties on the document.

Submissions, which should be entitled “Public Consultation” can be sent by;

- Email to: public_consultation@psa.gov.ie
- Fax to: 00353-62-31731
- Post to: Public Consultation
Private Security Authority
Davis St
Tipperary Town
Co. Tipperary

The closing date for receipt of responses is Friday, the 6th December 2013.

The Authority may publish submissions received in whole or in part in future documents. If submissions contain confidential information, such information should be clearly and unambiguously marked as confidential.

4th November 2013

CONTENTS

1.	SCOPE	4
2.	DEFINITIONS	5
3.	ORGANISATION	8
	3.1 Ownership	8
	3.2 Finances	9
	3.3 Insurance	9
	3.4 Premises	9
	3.5 Organisation Information	10
	3.6 Quotations in pursuance of Contracts or Business	11
	3.7 Compliance with Legislation	11
4.	STAFFING	11
	4.1 Selection and Pre Employment Screening	11
	4.2 Terms of Employment	16
	4.3 Code of Conduct	17
	4.4 Identification	17
	4.5 Uniform	18
	4.6 Threats and Violence	18
5.	TRAINING	19
	5.1 Training Policy and Responsibility	19
	5.2 Induction Training	20
	5.3 Venue Related Training	20
	5.4 Basic Training	20
	5.5 Trainers and Training	21
	5.6 Specialist Training	21
	5.7 Refresher Training	21
	5.8 Supervisory and Management Training	21
	5.9 Training Records	22
6.	OPERATIONS	22
	6.1 Risk Assessments	22
	6.2 Event Security Staffing Requirements	23
	6.3 Command and Control System	24
	6.4 Command and Control System Manual	25
	6.5 Command and Control System Controller	26
	6.6 Command and Control System Training	27
	6.7 Incident Reporting	27
	6.8 Operations Records	28
	6.9 Assignment Instructions	28
	6.10 Security of Information and Access Media	29
	6.11 Vehicles and Drivers	29
	6.12 General	30
7.	COMPLIANCE WITH PSA LICENSING	30
	7.1 Compliance With Standards	30
	7.2 PSA Licensing Requirements	31
ANNEX A		32
	Screening Forms	32
ANNEX B		36
	RISK ASSESSMENT GUIDELINES	36

1. SCOPE

This standard provides a specification for compliance with licensing by the Private Security Authority and applies to contractors seeking licences in the following sectors, Door Supervisor (Event Security) and Security Guard (Event Security).

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

- The inspection and compliance 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 (PSA) and those seeking a licence from the PSA must comply with this Requirements Document. Only certification bodies approved by the PSA may provide certification services for licensing purposes. Contractors should check the PSA website, 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 the contractors certification process between the PSA and the contractor's certification body. Where a contractor fails to comply with the requirements of this document, 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.

This document is for the purpose of licensing by the Private Security Authority and should not be interpreted as meeting any other statutory obligations of a contractor.

2. DEFINITIONS

2.1 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.

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

2.3 Assignment Instructions. Set of written instructions drawn up by the organisation in agreement with the customer specifying the contractual duties.

2.4 Authorised Certification Body. A certification body authorised by the PSA to provide certification services in respect of event security services.

2.5 Authorised Officials. Personnel of the PSA, Certification Bodies authorised by the PSA or 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 event security employees to meet the mandatory training requirements in respect of PSA licensing.

2.7 Check-in Call. Routine communication to verify the location and status of an event security officer on an assignment.

2.8 Client. Individual or organisation retaining a security service covered by this standard to carry out agreed services, responsible for remunerating the organisation in accordance with an agreed contract or other form of oral or written agreement to provide such services.

2.9 Command and Control System. Secure facility where operational procedures are monitored and/or managed.

2.10 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.

2.11 Controller. The person fulfilling the role and duties of a Command and Control System Officer.

2.12 Door Supervisor (Event Security) The provision of any of the following functions at, in or in the vicinity of any premises or any other place where a public or private event or function is taking place or about to take place –

- (a) controlling, supervising, regulating or restricting entry to the premises or place,
- (b) controlling or monitoring the behaviour of persons therein,
- (c) removing persons therefrom because of their behaviour;

2.13 Event. A gathering of people either at public or private locations for entertainment, social performance or other purposes e.g. sporting, trade events or social functions, held within temporary or fixed, indoor and outdoor locations on a regular, occasional or once off basis. Event Security is the provision of security services at such an event.

2.14 Entertainment Area. The specific area of a venue where the entertainment or social performance takes place and where the provision of a security service is undertaken by a Door Supervisor (Event Security) provider. The Entertainment Area includes areas where alcohol and food are served.

2.15 Identity Badge. The identification card or licence card held by the employee to be visibly worn (subject to certain exemptions prescribed by the PSA) by operational security staff whilst on duty, the design and conditions of which are as specified from time to time by the PSA.

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

2.17 Licence Card. The official identification card issued by the PSA to each individual employee licence holder to verify his or her licence status.

2.18 Organisation. A limited or unlimited company, a partnership or sole trader providing services relating to event security for which a relevant and applicable PSA licence is required.

2.19 Periphery Area. The specific area of a venue adjacent to or in the vicinity of the Entertainment Area where the provision of a security service is undertaken by a Security Guard (Event Security) provider. The Periphery Area includes car parks, accommodation areas, venue perimeter and approaches, and any other location not within the Entertainment Area.

2.20 Primary Service. The service provided for which the

organisation and the client have agreed remuneration will be paid and a service or services will be provided, all or part of which will compromise a security service covered by this standard.

2.21 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.

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

2.23 Qualified Trainer. Means a trainer with the following minimum qualifications:

- a) A Level 5 Security Industry Trainer Award, or
- b) A Level 6 Train the Trainer Award together with a Level 4 Minor Award in Guarding Skills or Door Security Procedures or Security Industry Awareness, or
- c) A Level 6 Special Purpose Award in Training and Development together with a Level 4 Minor Award in Guarding Skills or Door Security Procedures, or
- d) A qualification or award which is equivalent to either a), b) or c) above on the National Framework of Qualifications.

Note: Security Industry Awareness award is abolished from December 2012.

2.24 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.

2.25 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.

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

2.27 Security Guard (Event Security). The provision of patrols or other protective services in relation to persons or property in any premises or any other place where a public or private event or function is taking place or about to take place, including the

controlling, supervising, regulating, restricting and directing the movements of persons at an event or function.

Note: Security Guard (Event Security) does not include guarding or protective services provided in relation to a specific individual or specific individuals.

2.28 Security Guard (Event Supervisor). A person who controls, supervises, regulates, restricts or directs the movements of event security staff, whether in vehicles or otherwise and who is in communication with the command and control system.

2.29 Training Administrator. Person appointed to supervise and record all aspects of training within the organisation.

2.30 Venue. Any location where an Event takes place including service areas.

2.31 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 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 shall be disclosed to an authorised person on request.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.1.6 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 that a valid tax clearance certificate is held on site at the address recorded on the Private Security Services Licence during the term of the licence.

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 cash flow statement for the last accounting period. For new organisations a cash flow forecast for the first 12 months of business shall be provided.

3.3 Insurance

3.3.1 All insurance 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
- Motor insurance
- Deliberate act
- Fidelity
- Defamation
- Efficacy
- Consequential loss of keys
- Wrongful arrest
- 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 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 (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)** Level of response to be provided and the means for reporting and exchanging necessary operational information.
- (f)** Safety statement.
- (g)** Details of complaints procedures and complaints management procedures
- (h)** 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 e-mail delivery of the contract or general terms and conditions 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 or general terms and conditions.

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 by a principal of the organisation, of its compliance with all relevant legislation and shall state specifically its compliance, where relevant, with the following:

- Health, Safety 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.

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

- The PSA
- National Employment Rights Authority
- Authorised Certification Body

3.7.2 Notwithstanding the requirements of sub-clause **3.6.1** the organisation shall hold at its premises verification of compliance with current legally enforceable agreements or legislation in respect of rates of pay and all associated conditions.

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 participation in, access to details of, or knowledge of security duties 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 employment until screening is completed.

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 Persons employed for security duties as Door Supervisor (Event Security) personnel or Security Guard (Event Security) personnel shall not be less than eighteen years of age. Persons beyond fifty-five years of age shall be required to undergo an annual medical examination to ensure their fitness for the duties to which they may be assigned.

4.1.1.11 Persons employed for security duties as Security Guard (Event Supervisor) personnel shall not be less than twenty-five years of age and shall have a minimum of 3 years experience as either a Door Supervisor (Event Security) or Security Guard (Event Security) operative. Persons beyond fifty-five years of age shall be required to undergo an annual medical examination to ensure their fitness for the duties to which they may be assigned.

4.1.1.12 Full screening for the period covered under **4.1.1.9** above shall apply except in the following circumstances:

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 under a standard accepted for licensing by the PSA within the preceding five years and these screening records have (with each individual employees consent) been transferred to the current employer by the previous employer.

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 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 (but only with each individual employees consent) 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) Periods of unemployment
- (d) Applicant's current place of residence
- (e) Periods of education

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 of the applicant and the general 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) The level of occupational fluency in respect of reading, writing and oral communication in the English language.
- (e) The applicant's experience, if any, in providing a security service.

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 two attempts, in writing, by the organisation to obtain the continuous record referred to in this requirement.

4.1.3.2 Where initial references in respect of employment are taken by telephone the following procedures shall be used:

- (a) 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, Forms 2 for a suggested format).
- (b) 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).
- (c) The screening process shall not be regarded as complete until written evidence is obtained (this includes at least two attempts, in writing, required under 4.1.3.1 above).
- (d) 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 Subject to satisfactory screening and the provisions of **4.1.1.5**, all applicants for employment on operational duties shall be offered employment only when they have completed a questionnaire relating to their medical history and present general health.

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. Where an applicant holds a PSA licence this shall stand as evidence of the applicant having achieved the awards necessary for obtaining the licence.

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.

4.1.6 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 at the company 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 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 provisional basis shall be maintained, and in the case of those employed on a provisional basis, giving the dates on which provisional 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 twenty 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 Terms of employment shall include the following information:

- (a) Job title.
- (b) Effective start date.
- (c) Probationary period (if applicable).
- (d) Effective end date (if applicable).
- (e) Pay and Allowances.
- (f) Hours of work, days of work, shift frequency and shift variables.
- (g) Holiday entitlement.
- (h) Sick pay (conditions of payment) and pension entitlement.
- (i) Industrial injury procedure.
- (j) Employer's registered address.
- (k) Equipment to be supplied.
- (l) Disciplinary and grievance procedures.
- (m) Terms of notice and termination.
- (n) Collective Agreements (copies available) covering the employment.
- (o) Appeals procedure.
- (p) The Organisation's Health and Safety Statement.
- (q) The Organisation's Equality policy.
- (r) Workplace Bullying/Harrassment policy.
- (s) E-mail, Telephone and Internet 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) Remain at their place of work unless permission to leave is given by an authorised officer of the security provider or there is sufficient cause.
- (c) Ensure that all oral or written statements made by them, of whatever description, are true and accurate.
- (d) Maintain carefully all documents and ensure that any alterations, disposal, or erasure of documents is carried out only with proper authorisation.
- (e) Maintain confidentially on any matter relating to the employer or his clients either past or present.
- (f) Maintain a very high level of personal integrity, and be scrupulous when representing the employer's business.
- (g) Extend courtesy to persons encountered in the course of work, ensuring that any exercise of authority is only that required in connection with the employer's business.
- (h) Ensure that any actions taken by them are such as not to bring discredit on the employer, the client or fellow employees.
- (i) Wear the employer's uniform, and use his equipment and identification only with the employer's authority.
- (j) Ensure that they are not under the influence of, or consume, alcohol or restricted drugs whilst at work.
- (k) Immediately notify any conviction for a relevant criminal or motoring offence to the employer.
- (l) Ensure that they use employer's equipment or facilities and client's equipment or facilities only with authorisation.
- (m) Continuously satisfy the requirements of PSA licensing.
- (n) 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.

4.5 Uniform

4.5.1 The organisation shall provide each employee 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 patrons and other staff or venue employees. Lettering shall clearly indicate the word "SECURITY" in a prominent position on a high visibility background.

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

4.5.4 Each uniform must contain a unique identity number on the front and back. The unique identity number shall be clearly visible when the uniform is worn in normal working environments.

4.5.5 The uniform must 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 Subject to normal wear and tear the organisation shall provide for renewal of uniforms.

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

4.5.8 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.

4.6 Threats and Violence

4.6.1 The organisation shall, as part of its risk assessment of the venue, assess the risks for violence that security 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.

4.6.2 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.

4.6.3 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.

4.6.4 In the case of identified risk of recurring violence, employees shall be given additional support by the employer. Work locations shall be chosen and equipped so that the risk of violence is minimized. It should be possible to call for help in case of violence or in a situation where the potential for violence is clear and imminent.

4.6.5 Tasks involving a high risk of violence shall be identified in the risk assessment and shall be carried out by two or more operatives working together.

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

4.6.7 An employer 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.

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.

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 Venue Related Training

5.3.1 Facilities shall exist for familiarisation procedures and training of newly recruited employee's going to a first assignment or existing employees transferring between assignments. Such training shall be carried out by a qualified trainer or experienced members of staff.

5.3.2 A detailed venue-specific training plan in accordance with relevant assignment instructions shall be documented. The training plan shall reflect the required knowledge and skills necessary to carry out the particular duties associated with each venue.

5.3.3 Once deployed at a venue, employees shall be trained in accordance with the requirements set out in the detailed venue-specific training plan.

5.3.4 The training covered by 5.3.3 shall be delivered by a competent member of staff and shall be recorded and this record shall be retained.

5.4 Basic Training

5.4.1 The organisation shall ensure that all relevant operational security staff are qualified for each service activity provided e.g.

- Door Supervisor (Event Security)
- Security Guard (Event Security)

5.5 Trainers and Training

5.5.1 Except where otherwise expressly provided for within this standard, all training shall be delivered by qualified trainers, as defined in **2.23** of this document, during the course of employment with the organisation.

5.5.2 For delivery and assessment of all training conducted during the period of employment of the individual with the organisation, the employer shall satisfy itself as to the competency and qualifications of trainers.

5.6 Specialist Training

5.6.1 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.

Note: Examples of specialist training required would include command and control system operations, searches, removal of persons, etc.

5.6.2 Where risks are identified, in the course of carrying out a risk assessment under **6.1.1**, additional training, specific to these risks, shall be provided where basic training has not addressed the nature of the risk(s) involved.

5.7 Refresher Training

5.7.1 The training policy shall include provision for refresher training to be provided to operational staff of a duration and content sufficient to

(a) maintain the knowledge and skills of the staff concerned,

and

(b) address any developments in methods, procedures, technology or relevant legislation since the staff member was last subject to structured training.

5.8 Supervisory and Management Training

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

5.9 Training Records

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

5.9.2 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.

5.9.3 Verification of all training shall be available for inspection by authorised bodies at the organisation's premises.

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

6. OPERATIONS

6.1 Risk Assessments

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

6.1.2 The risk assessment shall be accordance with the risk assessment guideline contained in Annex B of this document.

6.1.3 A risk control plan shall be prepared and incorporated into the Event Security Management Plan.

6.1.4 An Event Security Management Plan shall be drafted in consultation with relevant stakeholders and in keeping with contractual obligations, the plan shall be provided to the client and include as a minimum reference to each of the following:

- (a) Numbers of staff and general designation, where defined e.g.
 - Command and Control System team
 - Supervisors
 - Staff for normal security duties
 - Pit crews
 - Access control teams
 - Perimeter security teams
 - Incident response teams
 - Search teams

- (b) Crowd management including policy and procedures on searches and removal of persons
- (c) Major incident planning
- (d) Identification of staff
- (e) Communications equipment
- (f) Traffic management
- (g) Control of entry.
- (h) Management of exits
- (i) Fire hazards and responses
- (j) Security of performance area(s)
- (k) Security of performance equipment
- (l) Security of moveable objects
- (m) Health and safety of its staff
- (n) Personal risk assessment of its staff
- (o) Site plan of the venue divided into zones (each zone to relate to the area of control of each Security Guard (Event Supervisor)).

6.1.5 All designated event security employees shall attend a pre-event briefing session the content of which shall relate directly to the event undertaken, the duration and subject matter of the briefing session depending upon the complexity of the venue and event.

6.1.6 In addition to the pre-event briefing session each event security employee shall receive written instructions on what their duties and responsibilities are.

6.1.7 Verification of the pre-event 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, countersigned and dated by the organisation's management.

6.1.8 A copy of the countersigned attendance register shall be attached to the Command and Control System Manual.

6.2 Event Security Staffing Requirements

6.2.1 The number of event security staff on duty at an event shall depend on the risk assessment and Event Security Management Plan and shall be determined in consultation with the Local Authority and An Garda Síochána.

6.2.2 Notwithstanding the requirements of sub-clause **6.2.1** the organisation shall provide as a minimum one Door Supervisor (Event Security) for 250 persons in permanent seats, stands or terraces and one Door Supervisor (Event Security) for 100 persons in all other areas.

6.2.3 Where an audience is predominantly under the age of 16 a doubling of the staffing requirements at **6.2.2** shall be required.

6.2.4 Door Supervisors (Event Security) shall be assigned in groups of 10 and the organisation shall assign one Security Guard (Event Supervisor) to control each group.

6.2.5 Security Guard (Event Security) shall be assigned in groups of 10 and the organisation shall assign one Security Guard (Event Supervisor) to control each group.

6.2.6 There shall be a reserve of event security staff of adequate numbers to provide for break periods and contingencies.

6.2.7 Each Security Guard (Event Supervisor) shall meet with his group in advance of the group commencing duty.

6.3 Command and Control System

6.3.1 Unless provided by the client, the organisation shall provide a command and control system at the venue. The command and control system shall be sound proof and suitable for all weather conditions.

6.3.2 The following minimum provisions shall apply for all command and control systems;

- (a) The command and control system shall be secure from interference, by unauthorised persons,
- (b) Access to the command and control system shall be restricted to the following persons;
 - The controller,
 - A representative of the client,
 - A representative of An Garda Siochana,
 - A representative of the local authority/emergency services,
 - A representative of the PSA,
 - Such other persons authorised by the controller to be present.
- (c) A record shall be maintained of all persons entering and leaving the command and control system,
- (d) Manning of the command and control system shall be consistent with the anticipated workload, the nature of the work and the requirements of the risk assessment,
- (e) The organisation shall maintain a copy of the risk assessment and command control system manual in the command and control system,
- (f) The command and control system shall be able to communicate with each Security Guard (Event Supervisor) and such other operational staff as is

- required for the efficient provision of the security service at the venue,
- (g) The command and control system shall control all CCTV cameras at the venue and shall be able to view all CCTV images in real time,
 - (h) The command and control system shall have sufficient communication channels including telephone lines, mobile phone coverage and wireless broadband to handle any emergency,
 - (i) The command and control system shall have an emergency power supply,
 - (j) A daily register of all event security staff on duty shall be available at the command control system, detailing as a minimum:
 - o the total number of staff designated as event security,
 - o full name of each event security staff member,
 - o PSA Employee licence number for each event security staff member ,
 - o the unique identity number of the uniform allocated to each staff member,
 - o the location of and duties assigned to each staff member.
 - (k) The equipment, furnishings and layout of the command and control system shall be consistent with the efficient operation of the system,
 - (l) Heating, lighting and ventilation shall be provided to ensure a reasonable working environment.

6.4 Command and Control System Manual

6.4.1 For each Command and Control System there shall be a Command and Control System Manual. The Command and Control System Manual shall be produced as part of the risk assessment for a venue.

6.4.2 The Command and Control System Manual shall include the following;

- (a) The Event Security Management Plan for the venue,
- (b) The name and contact details of the Event Controller,
- (c) Guidance for controllers in dealing with all foreseeable contingencies,
- (d) The assignment instructions agreed between the organisation and client,
- (e) the organisation's escalation policy in the event of a major incident,
- (f) site plan of the venue divided into zones with the name of each Security Guard (Event Supervisor) for each zone.

- (g) Information on the provision, or procurement, of assistance or advice in routine and emergency situations,
- (h) The phone number and location of the various emergency services,
- (i) The emergency phone number and contact details of the organisations senior manager responsible in the event that an incident needs to be escalated to a more senior official,
- (j) The emergency phone number and contact details of the clients senior manager responsible in the event that an incident needs to be escalated to a more senior official,
- (k) Comprehensive instructions outlining action to be taken on receipt of incident reports,
- (l) A copy of the daily register of all event security staff as set out at 6.3.2(j),
- (m) The countersigned pre-event briefing session attendance register.

6.4.3 The organisation shall review the Command and Control System Manual for fixed location venues once every twelve months or following a major incident, whichever is sooner or where requested to do so by the PSA.

6.4.4 The organisation shall produce a Command and Control System Manual for temporary location venues as part of the risk assessment.

6.4.5 Copies of the Command and Control System Manual shall be made available to;

- The client,
- An Garda Síochána,
- The local authority/emergency services,
- The PSA.

6.5 Command and Control System Controller

6.5.1 The organisation shall appoint a suitability qualified person who shall be responsible for the management of all security services at the venue. This person is referred to in this document as the Controller and shall be responsible for all tasks assigned to the Controller in this document.

Note. Persons referenced as the Chief Steward in Codes of Practice issued by the Department of Education may act as the Controller.

6.5.2 The Controller shall be in command of the Command and

Control System at all times except where provided for at **6.5.3**.

6.5.3 The Controller shall pass command of the Command and Control System to a member of the emergency services in the event of a major incident or if instructed to do so by the emergency services. The time, name of person taking over command and the reason for the change shall be recorded in the Incident Report.

6.6 Command and Control System Training

6.6.1 All command and control staff shall be required to partake in practice drills for responses to emergency situations which might arise. Such drills shall take place at least once every 12 months for fixed locations and prior to the commencement of the event at temporary locations. The outcome(s) of the drills shall be documented and recorded.

6.7 Incident Reporting

6.7.1 All incidents shall be handled by the Controller 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) Action taken, including onward reporting.
- (e) Further action to be taken.
- (f) Where possible, names and addresses of all relevant persons present.

6.7.2 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 company'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.

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

6.8 Operations Records

6.8.1 All operational staff shall be made aware in writing of the identity of the 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 A record of all reported incidents shall be maintained for a minimum of three years.

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

6.8.4 A record of all check-in calls to the command and control system shall be kept for a minimum of three years.

6.8.5 A facility shall exist for the checking and reviewing of reports and reporting procedures periodically by senior management of the organisation.

6.8.6 Records shall be maintained for a period not less than three years for each venue, which shall include the service provided and the name, PSA licence number, uniform unique identity number, identification number or works number of any person employed at such venue. 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.

6.9 Assignment Instructions

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

6.9.2 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) or delivery to the client and any subsequent correspondence.

6.9.3 The assignment instructions shall be available in the command and control system manual and a copy shall be available to the client.

6.9.4 Assignment instructions shall include:

- a) The Risk Assessment,
- b) The Command and Control System Manual,
- c) The procedure for contacting the organisation's command and control system,
- d) Details of the service to be provided at the venue on the clients behalf including
 - i. the number of personnel involved in the assignment and their responsibilities,
 - ii. hours for which the service is to be provided and handover instructions at start and end of service,
 - iii. facilities, vehicles or equipment provided by client,
 - iv. safety statement,
 - v. welfare facilities for staff.
- e) A site plan of the venue,

6.10 Security of Information and Access Media

6.10.1 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.

6.10.2 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.

6.10.3 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.

6.11 Vehicles and Drivers

6.11.1 All operational vehicles shall clearly display the organisation's name, badge or logo and telephone number(s).

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

6.11.3 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. Copies of all driving licences shall be held on the employee's file.

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

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

6.12 General

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

6.12.2 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 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.

7.1.2 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.

7.1.3 Organisations shall give their permission to the approved certification body to provide the PSA with information in accordance with provisions **7.1.4** and **7.1.5**.

7.1.4 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.

7.1.5 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 by or 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 During the term of the licence organisations shall comply with all relevant 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

7.2.3 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. In the case of a partnership, change in partners.
- c) Change of ownership of the company. In the case of a body corporate this includes a change in any shareholding above 5%.
- d) Change of address from which the security service is being provided.
- e) Change of registered address if this is different from address at d) above.
- f) Change in the legal status of the licence holder.
- g) 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.

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 event security.

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 event 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 event 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

	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 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

RISK ASSESSMENT GUIDELINES

EVENT SECURITY

1. Scope

The purpose of these guidelines is to outline the process to be applied by Private Security Authority Licensed Contractors when undertaking a Risk Assessment as required by Section 6.1 of the PSA Standard for Event Security

2. Introduction

Risk assessment and management underlies the duties of PSA Licensed Contractors under the provisions of the PSA Standard. Under this standard 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 process which should be undertaken along with some of the factors that should be considered by contractors when identifying hazards, 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 approved Certification Bodies.

The PSA standard specifies that a risk assessment shall be undertaken for each venue. The extent and level of documentation of hazard 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 health and safety and in risk assessment and who has the ability to assess all potential hazards at a venue.

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

3. Event Security Risk Management (SRM)

The implementation of a Security Risk Management Process (SRMP) will provide a mechanism which ensures that hazards and associated 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 hazards;
2. assess the security risk arising from the hazard 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 Hazards

Hazard identification relevant to a particular aspect of a contractor's operation (e.g. clients requirements, service provision, venue, nature of performance, public interface, recorded incidents, mobile patrols, 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. outdoor, indoor, sporting arena, purpose built venue, public space, etc) and the risk associated with such locations.

Attention should also be given to potential hazards which could arise as a result of abnormal or emerging situations (e.g. electrical/technical failures, crowd violence, weather alerts, etc).

3.1.1 Hazard Identification process

The activities used to identify hazards 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 clients venue;
- conducting assessments of public interface;
- conducting assessments of past events at which the performers participated;
- 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 An Garda Síochána, government bodies/local authorities/emergency services and risk assessment consultants on likely security hazards.
- conducting assessments of crowd dynamics;

- conducting assessment of cultural behaviour;
- conducting assessment of access/egress points;
- assessing temporary structures and movable items.

Potential security hazards shall be identified in respect of all aspects of a contractor's security operations and in the context of the security service provided. These aspects of operations shall include but are not limited to the following:

- the tasks performed;
- the locations involved;
- the command and control system;
- members of the public present;
- possible collective behaviour of the public;
- the different roles of the contractor's staff;
- the communication methods used;
- the time of day that the work is to be performed;
- use of Personal Protective Equipment (PPE) and any other equipment or technologies required;
- work practices and procedures, shift working arrangements and other fatigue and stress related hazards;
- manual handling tasks;
- environmental factors (e.g. outdoor, terrain, weather, lighting, traffic and pedestrian flow, intoxication, etc).

3.2

Assessing the Security Risk

After the identification of a hazard, the contractor shall assess the risk posed by the hazard. This informs the likelihood of an identified hazard 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 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;
- venue location and layout;
- staffing levels required to safely perform the work;
- type of service required (taking account of public interface crowded numbers, nature of performance).

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 hazards 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 hazards. Notwithstanding the obligation of contractors to comply with the PSA Standard, 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 hazard is not possible.

3.3.2 Substitution of Risk

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

3.3.3 Hazard Isolation

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

3.3.4 Minimizing Exposure to Hazard

The exposure to the hazard 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;
- 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 annually or more frequently if 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 10 provides a basic format for all risk assessments referred to and required within the PSA Standard. A contractor may substitute another format for the risk assessment template provided it has, as a minimum, the headings provided in the template on page 10. The template will assist contractors to:

- identify the hazards,
- 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 hazards 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.

Risk Assessment Template

Company Name:				Project:			
Location to be assessed:		Ref:		Date:			Page
Ref	Activity /Element	Actual/Potential Hazards	Risk Rating			Existing Controls	Further Controls/Actions Required
			L	S	R		
1							
2							
3							
4							
5							

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)
 S = Potential Severity (rating is within the range of 1 to 5 with 1 being the least severe consequences and 5 being the most severe consequences)
 R= Risk (this is arrived at by multiplying the numerical values assigned to the likelihood and potential severity respectively as above),
 i.e. $L \times S = R$ on a scale of 1 to 25 with 25 being highest risk