# QCI – CAPSI Voluntary Initiative
# Security Agencies Rating Scheme

# Technical Criteria

## Requirements for
## Private Security Agencies

# Table of Contents

## 0. Introduction

**0.1** This document specifies the requirements for a quality management system for the management, staffing and operation of a Private Security Agency providing security guarding services on a static site and/or mobile and patrol basis, at different capability levels.

**0.2** The purpose of this Technical Criteria – 'Requirements for Private Security Agencies' is

1) Rating and Certification of Private Security Agencies
2) Improvements, and
3) Competitive Differentiation

The criteria provides clients of security services with an objective, consistent means of evaluating the capabilities of potential Private Security Services provider. It offers guidance to Private Security Agencies that will help them improve their capabilities. It also gives Private Security Agencies a publicly available standard to use to differentiate themselves from their competitors.

**0.3** These capability levels can be used for rating and a basis of voluntary certification and demonstrating the ability of the Private Security Agency to consistently provide security services that meet customer and applicable statutory and regulatory requirements. The ratings and certification would enable a Private Security Agency to provide assurance to the stakeholders of capability at subscribed level and also provide a stepped approach to improvements.

**0.4** The improvement path as defined in these capability levels starts with a desire to provide security services, and continues to the highest level, demonstrating an ability to sustain trust and excellence.

**0.5** Requirements for the following capability levels of a Private Security Agency are defined:

**Level 1 – One Star – Meeting Compliance Requirements**

**Level 2 – Two Star – Established Compliance Management**

**Level 3 – Three Star – Consistent Operations**

**Level 4 – Four Star – Sustained Performance**

**Level 5 – Five Star – Assured Quality**

**Level 6 – Six Star – Trusted Excellence**

**Level 7 – Seven Star – Professionally Managed Security Operations**

**0.6** The capabilities of Private Security Services not falling in a Capability Level defined above may vary widely. Some may have not implemented any of the requirements as defined in this Technical Criteria and are likely to be high risk for their customers because they often promise more than what they can deliver. Other PSA's may have some of the requirements implemented, including those at level 3 or 5. Because these PSA have not implemented all the requirements at level 1 and may still meet customer's needs successfully, but they will still be

at risk of failure in areas where they have not implemented the necessary requirements.

**0.7** All requirements at a particular level of this document are generic and are intended to be applicable to all private security agencies, regardless of type, size and services provided. This Technical Criteria does not apply to all security services, for example cash-in-transit services, secure parcel services, close protection services, event stewarding and the management and operation of -surveillance system.

**0.8** The requirements applicable for a particular level are the requirements defined for that particular level and of all lower levels. However, requirements of a higher level can be used by the PSA for guidance and improvements.

**0.9** Where any requirement(s) of this document cannot be applied due to the nature of an agency and its services, this can be considered for exclusion.

If any requirement(s) of this document is (are) not applicable at a particular capability level due to the nature of the services for which the quality management system is applied, the agency does not need to include such a requirement(s) in its quality management system and appropriate justification shall be recorded, provided such exclusions do not affect the agency's ability, or responsibility, to provide services that meets customer and applicable statutory and regulatory requirements

## 1. Scope

**Level 1 – One Star – Meeting Compliance Requirements**
The Technical Criteria at this level specifies the requirements for of a Private Security Agency providing security guarding services on a static site and/or mobile and patrol basis, which needs to maintain and demonstrate **compliance** to applicable **statutory and regulatory requirements.**

**Level 2 – Two Star – Established Compliance Management**
The Technical Criteria at this level specifies the requirements for of a Private Security Agency providing security guarding services on a static site and/or mobile and patrol basis, which needs to maintain and demonstrate **established systems** for **continued compliance** to applicable **statutory and regulatory requirements**.

*The Private Security Agencies at Capability Level 2 demonstrate establishment of a compliance management system by effectively implementing all of* ***level 1*** *requirements for* ***two or more consecutive Certification Cycles*** *covering a period* ***at least three years****. There are* ***no additional requirements*** *to reach Level 2.*

**Level 3 – Three Star – Consistent Operations**
The Technical Criteria at this level specifies the requirements for a **Private Security Services Management System (PSSMS)** for the management, staffing and operation of a Private Security Agency providing security guarding services on a static site and/or mobile and patrol basis, which needs to demonstrate its ability to **consistently provide security services** that meet **customer** and applicable **statutory and regulatory requirements**.

**Level 4 – Four Star – Sustained Performance**

The Technical Criteria at this level specifies the requirements for a **Private Security Services Management System (PSSMS)** for the management, staffing and operation of a Private Security Agency providing security guarding services on a static site and/or mobile and patrol basis, which

(a) needs to demonstrate its ability to consistently provide security services that meet customer and applicable statutory and regulatory requirements.

(b) Needs to demonstrate **measurable, sustained, and consistent operational performance**

*The Private Security Agencies at Capability Level 4 demonstrate Sustained Performance by effectively implementing all of **level 3** requirements for **two or more consecutive Certification Cycles** covering a period **at least three years**. There are **no additional requirements** to reach Level 4. Effective implementation of all the operational requirements shows an ability to sustain operational performance over time.*

**Level 5 – Five Star – Assured Quality**

The Technical Criteria at this level specifies the requirements for a **Quality Management System (QMS)** for the management, staffing and operation of a Private Security Agency providing security guarding services on a static site and/or mobile and patrol basis, which

(a) Needs to demonstrate its ability to **consistently provide security services** that meet **customer** and applicable **statutory and regulatory requirements**.

(b) Aims to **enhance customer satisfaction** through the effective application of the system, and the **assurance of conformity** to customer and applicable statutory and regulatory requirements.

**Level 6 – Six Star – Trusted Excellence**

The Technical Criteria at this level specifies the requirements for a **Quality Management System (QMS)** for the management, staffing and operation of a Private Security Agency providing security guarding services on a static site and/or mobile and patrol basis, which

(a) Needs to demonstrate its ability to **consistently provide security services** that meet **customer** and applicable **statutory and regulatory requirements**.

(b) Aims to **enhance customer satisfaction** through the effective application of the system, and the **assurance of conformity** to customer and applicable statutory and regulatory requirements.

(c) Needs to demonstrate **measurable, sustained, and consistent performance excellence and improvements**

*The Private Security Agencies at Capability Level 6 demonstrate Trusted Excellence by effectively implementing all of **previous level** requirements for **two or more consecutive Certification Cycles** covering a period **at least three years**. There are **no additional requirements** to reach Level 6. The services can be trusted as effective, continued, implementation of all the requirements shows an ability to sustain excellence throughout the organization over time.*

**Level 7 – Seven Star – Professionally Managed Security Operations**

The Technical Criteria at this level specifies the principles and requirements for a **Security Operations Management System (SOMS)** for organizations conducting or contracting security operations and related activities and functions while demonstrating:

a) conduct of **professional security operations** to meet the requirements of **customer** and other **stakeholders**;

b) demonstrate its ability to **consistently provide services** that meet **customer needs** and are in **conformance** with applicable **international, national and local laws** and **human rights requirements**

c) **consistency** with **voluntary commitments** to which it subscribes

## 2 Normative references

The following referenced documents are necessary for the application of this document:

(a) Private Security Agencies (Regulation) Act,2005 (Herein after referred to as The Act)
(b) Private Security Agencies Central Model Rules,2006 (Herein referred to as The Model Rules)
(c) ISO 9001:2015 Quality management systems - Requirements
(d) ISO 18788:2015 Management system for private security operations — Requirements with guidance for use

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

### 3.1 Assignment instructions

Operational document detailing site-specific contractual duties

### 3.2 Routine Communication

Routine communication to verify the location and status of a security guard on an assignment

### 3.3 Competent person

Person. suitably trained and qualified by knowledge and practical experience, and provided with the necessary instructions, to enable the required task(s) to be carried out.

### 3.4 Contract agreement

A specific type of agreement that meets certain requirements designed to create legally binding obligations between parties.

### 3.5 Control Centre

Location where operational procedures are monitored and/or managed

### 3.6 Controller

Person designated to monitor controlCentre operations and communications

### 3.7 Customer

Individual or body obtaining the services of the organization

### 3.8 Key(s)/access system
Tool or system allowing authorized access to a customer's property

### 3.9 Keyholding
Service whereby the organization holds keys to a customer's premises and/or equipment and vehicles for use as agreed in the contract or as directed

### 3.10 Mobile patrol
Security services provided by security guardstravelling to multiple sites physically distant from one another, within a defined period of time/or responding to a call

### 3.11 Principal
Owner, partner, board director or other executive in the private sector, or a managing executive officer of the agency in the public sector or a not-for-profit organization

### 3.12 Security Services Policy
Intentions and direction of the PSA, related to security services, as formally expressed by its principal

### 3.13 Quality
Degree to which a set of inherent characteristics of the security guarding services fulfils requirements

Note 1: The term "quality" can be used with adjectives such as poor, good or excellent.

Note 2: "Inherent", as opposed to "assigned", means existing in the security guarding services

### 3.14 Secure facility
Any vulnerable area which is adequately protected commensurate with the threat level

### 3.15 Security guard
Person who performs duties at a static site or on a mobile patrol

### 3.16 Service level agreement (SLA)
An agreement between a PSA (either internal or external) and the customer that defines the level of service expected from the PSA.

Note. SLAs are output-based in that their purpose is specifically to define what the customer agrees to receive.

### 3.17 Site
Property, assets, life covered by the contract.

### 3.18 Site Security In-charge
Any rank under contract responsible for site security.

### 3.19 Duty Post
Fixed, patrol, mobile locations or premises where the assigned individual performs his given instructions.

### 3.20 Supplier

Individual or company (and the persons employed, including all levels of subcontractor, by that individual or company) that supplies the organization with equipment, material and/or personnel which is used in providing the service to the customer

### 3.21 Takeover

Assuming contractual/ assigned responsibilities

### 3.22 Private securityagency (PSA)

A person or body of persons other than a government agency, department or organization engaged in the business of providing private security services or providing private security guards to any industrial or business undertaking or a company or any other person or property;

Note. PSA is also being referred as agency here in-after in the document.

## 4. Context of the Private Security Agency

### 4.1 Understanding the agency and its context

**Level 1:** The PSA shall determine external and internal issues, such as those related to compliance risks, that are relevant to its purpose and that affect its ability to achieve compliance to applicable statutory and regulatory requirements.

In doing so, the organization should consider a broad range of external and internal aspects, such as the regulatory, social and cultural contexts, the economic situation and the internal policies, procedures, processes and resources.

**Level 3:** The PSA shall determine external and internal issues, such as those related to compliance risks, that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its private security services management system.

The organization shall monitor and review information about these external and internal issues

**Level 5:** The requirements specified in 4.1 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 4.1 of ISO 18788:2015 applies.

### 4.2 Understanding the needs and expectations of interested parties

**Level 1:** The PSA shall determine:

- the interested parties that are relevant to achieve compliance to applicable statutory and regulatory requirements;
- the requirements of these interested parties.

**Level 3:** The PSA shall determine:

- the interested parties that are relevant to the private security services management system;
- the requirements of these interested parties.

**Level 5:** The requirements specified in 4.2 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 4.2 of ISO 18788:2015 applies.

### 4.3 Determining the scope of the private security services management system

**Level 1:** The PSA shall establish and determine the boundaries and applicability of the compliance to applicable statutory and regulatory requirements.

*NOTE The scope of the compliance system is intended to clarify the geographical and/or organizational boundaries to which the compliance system will apply, especially if the organization is a part of a larger organization at a given location.*

When determining this scope, the PSA shall consider:

- the external and internal issues referred to in 4.1;
- the requirements referred to in 4.2 and 4.5.1.

The scope shall be readily available as documented information.

**Level 3:** The PSA shall establish and determine the boundaries and applicability of the private security services management system.

When determining this scope, the PSA shall consider:

- the external and internal issues referred to in 4.1;
- the requirements referred to in 4.2 and 4.5
- the services of the organization.

The scope shall be readily available as documented information. The scope shall state the types of services covered, and provide justification for any requirement of this Technical Criteria that the PSA determines is not applicable to the scope of its private security services management system

**Level 5:** The requirements specified in 4.3 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 4.3 of ISO 18788:2015 applies.

### 4.4 Private security services management system and its processes

**Level 1:** The PSA shall establish, develop, implement, evaluate, maintain and continually improve a management system, including the processes needed and their interactions, in accordance with this Technical Criteria, to achieve compliance to applicable statutory and regulatory requirements.

**Level 3:** The PSA shall establish, implement, maintain and continually improve the private security services management system, including the processes needed and their interactions, in accordance with the requirements of this this Technical Criteria.

**Level 5:** The requirements specified in 4.4 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 4.4 of ISO 18788:2015 applies.

### 4.5 Compliance Obligation

### 4.5.1 Legal Status

**Level 1:** The organization shall be registered in India and licensed for business of private security agency by the controlling authority of the state(s) in which it operates.

### 4.5.2 Identifying the Compliance Obligations

**Level 1:** The PSA shall systematically identify its compliance obligations and their implications for its activities and services. The PSA shall have processes in place to identify new and changed laws, regulations, codes and other compliance obligations to ensure on-going compliance.

The PSA shall document its compliance obligations in a manner that is appropriate to its size, complexity, structure and operations. The agency shall identify, document and comply with all applicable laws and regulations.

## 5 Leadership

### 5.1 Leadership and commitment

**Level 1:** The management shall demonstrate leadership and commitment with respect to achieving compliance to statutory and regulatory requirements by:
a) ensuring that policies, procedures and processes are developed and implemented to achieve compliance to applicable statutory and regulatory requirements;
b) ensuring that the resources needed for the compliance to applicable statutory and regulatory requirements are available, allocated and assigned;
c) communicating the importance of meeting statutory and regulatory requirements
d) establishing and maintaining accountability mechanisms, including timely reporting on compliance matters, including noncompliance;

**Level 3:** Management shall demonstrate leadership and commitment with respect to the development and implementation of the PSSMS and continually improving its effectiveness by:

- Ensuring that the security services policy and security services objectives are established and are compatible with the strategic direction of the organization.
- Ensuring the integration of the PSSMS requirements into the PSA's business processes.
- Ensuring that the resources needed for the PSSMS are available to establish, implement, operate, monitor, review, maintain and improve the PSSMS.
- Communicating the importance of effective security services management and of conforming to the PSSMS requirements and its legal responsibilities.
- Ensuring that the PSSMS achieves its intended outcomes(s).
- Directing and supporting persons to contribute to the effectiveness of the PSSMS.
- Promoting continual improvement.

NOTE *Reference to "business" in this criteria can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence*.

Management shall establish and maintain a Code of Ethics.

Management shall provide evidence of active leadership for the PSSMS by overseeing its establishment and implementation.

**Level 5:** The requirements specified in 5.1 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 5.1 of ISO 18788:2015 applies.

### 5.2 Policy

**Level 1:** The management shall establish a compliance policy that
- is appropriate to the purpose of the PSA;
- provides a framework for setting compliance objectives;
- includes a commitment to satisfy applicable statutory and regulatory requirements;

**Level 3:** Management shall establish a security services policy that:
- Is appropriate to the purpose of the PSA
- Provides a framework for setting security services objectives
- Includes a commitment to satisfy applicable legal and other requirements, including voluntary commitments to which the organization subscribes
- Includes a commitment to continual improvement of the PSSMS

The security services policy shall:
- Be available as documented information
- Be communicated within the organization
- Be communicated to all appropriate people working for or on behalf of the PSA
- Be available to stakeholders, as appropriate
- Be visible and endorsed by principal
- Be reviewed at planned intervals and when significant change occurs

**Level 5:** The requirements specified in 5.2 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 5.2 of ISO 18788:2015 applies.

### 5.3 Organizational roles, responsibilities and authorities

**Level 1:** Management shall ensure that the responsibilities and authorities for achieving compliance to statutory and regulatory requirements are assigned and communicated within the organization.

The organization's top management shall appoint from amongst its member a specific Nodal Officer(s), who, irrespective of other responsibilities, shall have defined roles, responsibilities and authority for:

a) ensuring that various requirements are established, implemented and maintained in accordance with this technical criteria; and
b) reporting on compliance with legal requirements to top management for review and as a basis for improvement.

The ultimate responsibility for compliance with the legal requirements related to private security services shall rest with the top management, or as specified in the applicable statute.

**Level 3:** Management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Management shall assign one or more individuals within the organization who irrespective of other responsibilities shall have defined competencies, roles, responsibilities and authority for:

(a) Ensuring that the PSSMS conforms to the requirements of this Criteria
(b) Ensuring that a PSSMS is established, communicated, implemented and maintained in accordance with the requirements of this criteria.
(c) Promoting awareness of PSSMS requirements throughout the organization
(d) Reporting on the performance of the PSSMS to top managers for review and as a basis for continuous improvement.

Management shall ensure that those responsible for implementing and maintaining the PSSMS have the necessary authority and competence to do so.

**Level 5:** The requirements specified in 5.3 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 5.3 of ISO 18788:2015 applies.

## 6 Planning

### 6.1 Actions to address risks and opportunities

**Level 1:** The PSA shall determine the compliance risks and plan actions to address the compliance risks to prevent, detect and reduce undesired effects.

**Level 3:** Management shall ensure adequate cashflow for its requirements. Latest two years audited balance sheet and profit and loss accounts shall be available at the head office.

The agency shall hold adequate insurance cover commensurate with the business undertaken and the number of persons employed, e.g. public liability, contractual, employer's liability and vehicle insurance etc.

**Level 5:** The requirements specified in 6.1 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 6.1 of ISO 18788:2015 applies.

### 6.2 Objectives and planning to achieve them

**Level 1:** The PSA shall establish its compliance objectives, consistent with the compliance policy, at relevant functions and levels for achieving compliance to statutory and regulatory requirements.

**Level 3:** The PSA shall establish security services objectives at relevant functions and levels.

The security services objectives shall:

a) be consistent with the security services policy;
b) be measurable (if practicable);
c) take into account applicable requirements;
d) be monitored;

e) be communicated;
f) be updated and/or revised as appropriate.

**Level 5:** The requirements specified in 6.2 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 6.2 of ISO 18788:2015 applies.

### 6.3 Planning of changes

**Level 5:** The requirements specified in 6.3 of ISO/IEC 9001:2015 applies.

## 7 Support

### 7.1 Resources

**Level 1:** The PSA shall determine and provide the necessary resources needed to implement and maintain the procedures for effective management of compliance with statutory and regulatory requirements related to security services.

Resources include financial and human resources, as well as access to external advice and specialized skills, organizational infrastructure, contemporary reference material on compliance management and legal obligations, professional development and technology.

The private security agency shall exhibit its statutory license/s as required, in a conspicuous place of its business, preferably, front office.

**Level 3:** The PSA shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the private security services management system.

#### 7.1.1 Premises

The agency shall have an administrative office(s) and/or operational centre(s) where records, professional and business documents, certificates, correspondence, files and other documents necessary for conducting business transactions shall be kept in a secure manner. The location of records and documentation, both local and centralized, shall be clearly defined.

#### 7.1.2 Control Centre

A place which is manned 24X7 to receive operational communication and to coordinate and escalate actions.

##### 7.1.2.1 Design

Control Centre shall allow the following functions, whether in combination or alone, to be performed:

(a) provision or procurement of assistance, information or advice for security guards (on static sites, mobile and patrols) and supervisors, in routine and emergency situations
(b) effective coordination of security personal (on static sites, mobile and patrols) and supervisors, by strict observance of documented, established telephone, radio or other communication procedures;

(c) All such coordination and escalations be appropriately recorded

**7.1.2.2 Emergency Facilities**

Where computerized and/or electronic systems are in operation, adequate resources shall be available to ensure continued operation of the control Centre in the event of power failure.

A communication line exclusive to the control Centre shall be provided. An emergency alternative means of communication shall be provided.

**7.1.2.3 Control Centre Procedures**

Method and contact details of reporting incidents or problems both within the agency and to the customer shall be defined and documented in a Control Centre procedure. The procedure shall clearly indicate the stages at which an incident shall be reported by the controller to the designated senior. A copy of the control centre manual shall be readily available within the control centre at all times.

The agency shall review and update Control Centre information at regular intervals (at least once every 12 months).

Records of incidents shall include the following:

(a) the date, time and location of the incident;
(b) the date and time of reporting, who reported and who received the report;
(c) details of the incident;
(d) action taken, including onward reporting;

**7.1.2.4 Information**

The controller should have immediate access to the following:

(a) the names, addresses and telephone numbers of supervisors and senior officials of the agency;
(b) emergency contact records (including telephone numbers) for all customers;
(c) telephone numbers of police stations within the operational area of the control centre and customer sites;
(d) useful telephone numbers (e.g. fire, electricity, ambulance, hospitalsetc.);
(e) a copy of the control Centre procedure;
(f) a register of keys that are held in the control Centre.

**7.1.2.5 Records**

The following records shall be kept:

(a) records of all reported incidents for a minimum of 3 months from the date of the incident. Entries shall be numbered serially and shall include the time and date of the incident and the name of the controller who has recorded the incident;
(b) A duty roster shall be maintained for all assigned persons in the control centre.

**7.1.2.6 Personnel**

The number of controllers in various control centers shall be commensurate with the expected workload.

Drinking water and toilet facilities shall be available. Suitable first-aid and fire-fighting equipment shall be provided.

**Level 5:** The requirements specified in 7.1 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 7.1 of ISO 18788:2015 applies.

## 7.2 Competence and Training

**Level 1:** The PSA shall:

a) determine the necessary competence for personnel performing work for it or on its behalf affecting compliance with legal requirements
b) provide training or take other actions to satisfy these needs
c) evaluate the effectiveness of the actions taken
d) maintain the associated records.

**Level 3:**

### 7.2.1 General

The agency shall have a clearly defined and documented training policy.

### 7.2.2 Induction training

The agency shall provide induction training in matters related to conditions of employment and organizational procedures to all employees. This induction training shall be additional to the basic job training described in **7.5.3**. Induction training shall be completed before the security guard and supervisor is appointed to an assignment.

*NOTE The content, timing and duration of induction training are left to the discretion of the agency.*

### 7.2.3 Basic training

All newly inducted security guards and supervisors mandatorily need to be trained and certified in accordance with the guidelines enumerated in The Act and Model Rules or as applicable in their jurisdiction.

### 7.2.4 Assignment-specific training

New guards and supervisors on assignment, or transferring between assignments, shall be given on-the-job training appropriate to the assignment and to the needs of the trainee and the customer.

### 7.2.5 Control Centre Training

Adequate training shall be provided as per requirement to the Controllers.

The competency of the controllers shall be assessed and any remedial training undertaken if required. Training records shall be maintained.

### 7.2.6 Supervisory training

Employees who have supervisory responsibilities shall be trained to a proficient standard by

suitably qualified and experienced persons in accordance with the NOS for the Job Role.

The competency of the supervisors shall be assessed and any remedial training undertaken if required. Training records shall be maintained.

**7.2.7 Progression training**

The agency should ensure suitable training of its employees to ensure their career progression.

**7.2.8 Take overs**

If employees are acquired through a takeover, the agency shall identify their training needs and address them with a specific training policy. This policy shall take practical work-related experience as well as qualifications into account.

Employees acquired through takeover shall not be exempt from the induction training.

**7.2.9 Refresher training**

The agency needs to have suitable policies to ensure periodic refresher training for its guards and supervisors or as specified under applicable PSARA Rules.

**7.2.10 Training records**

All training records shall be signed by the trainee, countersigned by the trainer and retained.

Where a certificate of training is provided by a recognized and recognized sector competent training organization, a copy shall be retained.

**Level 5:** The requirements specified in 7.2 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 7.1 of ISO 18788:2015 applies.

### 7.3 Awareness

**Level 1:** The PSA shall ensure that any person(s) performing tasks for it or on its behalf are aware of the importance of compliance with the legal requirements and the implications of departure from specified procedures.

**Level 3:** The PSA shall ensure that persons doing work under it's control are aware of:

a) the security services policy;
b) relevant security services objectives;
c) their contribution to the effectiveness of the private security services management system, including the benefits of improved performance;
d) the implications of not conforming with the private security services management system requirements.

**Level 5:** The requirements specified in 7.3 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 7.3 of ISO 18788:2015 applies.

### 7.4 Communication

**Level 1:** The PSA shall ensure that appropriate communication processes are established within the organization so that effective communication takes place for the various activities pertaining to management of compliance with legal requirements related to private security services.

The PSA shall ensure that appropriate communication processes are established for communicating the relevant information pertaining to compliance with legal requirements to the concerned regulatory authority and other stakeholders.

**Level 3:** The PSA shall determine the internal and external communications relevant to the private security services management system.

**Level 5:** The requirements specified in 7.4 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 7.4 of ISO 18788:2015 applies.

### 7.5 Documented Information

#### 7.5.1 General

**Level 1:** The PSA's compliance system shall include:
a) documented information recommended by this Technical Criteria;
b) documented information determined by the PSA as being necessary for compliance with statutory and regulatory requirements related to security services.

**Level 3:** The PSA's private security services management system shall include:
a) documented information required by this Technical Criteria;
b) documented information determined by the PSA as being necessary for the effectiveness of the private security services management system.

**Level 5:** The requirements specified in 7.5.1 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 7.5.1 of ISO 18788:2015 applies.

#### 7.5.2 Creating and updating

**Level 3:** When creating and updating documented information the PSA shall ensure appropriate:
- identification and description (e.g. a title, date, author, or reference or version number);
- format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
- review and approval for suitability and adequacy.

**Level 5:** The requirements specified in 7.5.2 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 7.5.2 of ISO 18788:2015 applies.

#### 7.5.3 Control of documented information

**Level 3:** Documented information required by the private security services management system and by this Technical Criteria shall be controlled to ensure:
a) it is available and suitable for use, where and when it is needed;
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

Separate records (hardcopy or electronic) should be maintained for each customer and employee.

The records should be held in a secure manner, but shall be easily accessible to authorized persons who have been screened.

Amended and/or updated records shall be identifiable by date and clearly distinguishable from previous versions.

Information stored in an electronic retrieval system shall be regularly backed-up. The back- up copies should be stored separately.

*NOTE Further information on the management of electronic data can be found in ISO/IEC 27001.*

Archived records shall be clearly indexed.

All records concerning a contract shall be maintained for at least 12 months or as specified by law after termination of the contract. Such records shall include:

**a)** all issues of assignment instructions;
**b)** daily registers and patrol and incident reports;
**c)** details of persons employed on the assignment.

An employee's basic records shall be kept for at least 7 years from the cessation of their employment.

*NOTE Minimum periods for retention of records can be reviewed if applicable for particular purposes, especially with regard to potential liabilities or regulations.*

**Level 5:** The requirements specified in 7.5.3 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 7.5.3 of ISO 18788:2015 applies.

**8 Operations**

**Level 1:** The PSA shall define and maintain appropriate controls for its activities relevant to legal requirements in order to ensure compliance with applicable statutory and regulatory requirements.

**Level 3: The requirements defined below in 8.1 to 8.7 are for Level 3 private security services operations.**

**Level 5:** The requirements specified in 8.1 to 8.7 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 8.1 to 8.8 of ISO 18788:2015 applies.

**Level 3 Requirements for Operations**

**8.1 Security services planning and control**

The PSA shall plan, implement and control the processes needed to meet the requirements for the provision of security services.

**8.2 Marketing**

### 8.2.1 Contacting prospective customers

When contacting prospective customers in order to sell security services by the authorized representative of the PSA shall carry authentic identification, both personal and of the agency.

### 8.2.2 Customer information

Agency shall provide prospective customers with the following basic information: -

(a) Brochure.

(b) Pre sale information as required by the prospective customer.

If requested by a potential customer, the following additional information shall be provided:

(a) Membership details of trade and professional associations.

(b) Details of licensing, if required.

(c) Reference sources for details of previous or current work carried out by the agency;

### 8.2.3 Site Survey

Prior to signing of the contract and SLA, the agency shall undertake an initial site survey. A report shall be made, identifying safety risks that the prospective customer is exposed to and preventive measures to be taken and manpower requirement assessed to mitigate the threats.

An authorized person(s) shall conduct initial site surveys and records shall be maintained to confirm that all relevant aspects have been considered. If possible, the report shall form part of the proposal to the customer; however, it shall be made clear that it is not intended to be a full assessment and recommendation for the foolproof security of a site.

Periodic review surveys shall be conducted to reassess the changes in security requirements, if any, in agreement with the customer and records thereof to be properly maintained.

If the customer declines to have initial site survey conducted, notes from the meeting with the customer shall be maintained.

Where existing assignments are taken over, the agency shall discuss with the customer and the previous service provider any implications with respect to the assignment.

### 8.2.4 Pre-Sales Operations

#### 8.2.2.1 Quotations

The customer requirements for security services and related statutory and regulatory requirements shall be understood and reviewed for ability to meet the requirements. .A clear signed quotation shall be provided by the PSA .

#### 8.2.2.2 Contracts

The contract document shall contain the following: -

(a) Mutually agreed terms and conditions between the PSA and the customer.

(b) Agreement on engagement of sub-contractors, if applicable

(c) Period of contract as agreed upon.

#### 8.2.2.3 SLA

The SLA shall comprise the following: -

(a) Mutually agreed service levels

(b) PSA must communicate the terms & condition for the concerned level of delivery.

Periodic checks shall be carried out to ensure delivery of security services as per SLA and reports of the checks shall be maintained. The progress against SLAs shall be communicated to the customer

#### 8.2.2.4 Contract and SLA records

Copies of records relating to the contract and SLA between the customer and the PSA shall be maintained.

### 8.3 Assignment instructions

#### 8.3.1 General

Assignment instructions for all duties and responsibilities shall be formulated in consonance with the contract, SLA and the customer and shall be available at the start of the contract.

Assignment instructions shall be agreed, and copies signed by the PSA and the customer.If the customer is reluctant to sign the assignment instructions, a copy shall be sent to the customer with a letter stating that, in the absence of indication to the contrary, these assignment instructions apply.

Security officers shall be familiar with the assignments on which they are working, and shall sign to confirm they have read and understood the assignment instructions.

#### 8.3.2 Content

The following details shall be included in the assignment instructions:

(a) the location, description and extent of the site or property;

(b) the agreed means of access;

(c) emergency procedures and lines of communication;

(d) frequency and method of communication with the control room, including the frequency of check calls;

(e) availability of customer's facilities, vehicles or equipment for use by security guards;

(f) accountability for and restrictions on a security guard actions;

(g) information on hazards, as identified during the initial site inspection (see**8.2**);

(h) the number of personnel involved in the assignment, and their individual duties and responsibilities, including:

I. working hours and any hand over requirements;

II. any patrol routes, and routine reporting points andtimes;

III. the management of CCTV surveillance systems and/or other specifically requested services;

IV. access control and searching procedures;

V. recordkeeping.

### 8.3.3 Amendments

Any permanent alteration to the instructions that results in changes to security guards' duties or operational requirements shall be agreed between the agency and the customer in writing.

Minor amendments shall be approved by the agency, and details sent to the customer.

Assignment instructions shall be amended and reissued as soon as practicable after changes have been agreed.

Temporary alterations shall be recorded in the site records (see **8.4.3**).

## 8.4 Site Operations

### 8.4.1 Information

Security guards shall be familiar with their general and specific site duties and responsibilities. These shall be fully documented in the form of assignment instructions (see **8.3**) and be available to each security guard at their assigned place of work.

Security personnel whilst on a mobile patrol shall have access to assignment instructions for each site to be visited.

### 8.4.2 Responsibilities

#### 8.4.2.1 Static Guarding Services

The prime responsibility of a security guard shall be to protect the customer's personnel, property and assets during hours of duty, to the extent possible.

Typical duties may include, but are not limited to:

a) regular tests of communication, safety and other equipment specified in the assignment instructions;
b) Regularly checking security of the site;
c) Monitoring movement of people, goods or transport;
d) Making check calls to ensure presence, alertness and response of the recipients of the call.
e) Receiving and handling external calls and enquiries;
f) Managing the movement of equipment and store for which the organization is responsible;
g) Taking out and depositing of the keys placed of his static post.
h) Attending and reporting incidents and emergencies.

#### 8.4.2.2 Mobile Patrol Services

The responsibility of a security guard on mobile patrol shall be to make prearranged visits to inspect the sites as detailed in the assignment instructions to ensure security of the site to the extent possible. He shall also patrol and he shall also react to any emergency which may develop to endanger to the security of sites as assigned to the patrol party.

*NOTE It might be necessary to consider conducting mobile patrols at random times and varying*

*the route to and from the sites to ensure that no patterns are established.*

### 8.4.3 Site records

The site records shall maintain as per SLA. However the following documents shall be maintained:

(a) records of incidents, which shall include the following:

I. the date, time and place of the incident;
II. nature of the incident (i.e. fire, flood or theft);
III. the date and time of reporting, and the name of the reporter;
IV. details of the incident;
V. action taken, including onward reporting;
VI. action to be taken;
VII. name (s) and address(es) of person(s) who witnessed the incident.

(b) All occurrences, incidents and actions taken shall be recorded, by time and date, in the register.

(c) changes in the assignment instructions;

(d) the signing-on and -off of the agency's personnel (including supervisory visits);

## 8.5 Control of keys

### 8.5.1 General

The security of keys held or managed by the agency shall be controlled in a manner that prevents its misuse.

A receipt shall be given for keys that are provided by the customer solely for the use of the agency. The agency shall be responsible for security and proper use of the keys till the site remains under the contractual assignment of the agency. Where keys are meant to be used for different location the record of the same shall be maintained by the agency.

### 8.5.2 Keys on static sites

When not in use, keys shall be kept in a secure manner. Each set of keys shall be stored ready for inspection at all times and shall be uniquely referenced with its details recorded in a key register.

The movement of keys shall be traceable and record shall be maintained.

If a key is not returned within the expected period, action shall be taken as specified in the assignment instructions.

### 8.5.3 Keys on mobile patrols

At the end of each patrol, keys that have been issued shall be returned and inspected to ensure correctness and safely of the keys. All key movements in and out of storage shall be recorded in the key register.

## 8.6 Staffing

### 8.6.1 General

The agency shall employ sufficient security and administrative staff, to fulfil its contractual obligations.

### 8.6.2 Security staff

#### 8.6.2.1 Deployment of Operational Staff

The Agency shall employ guards and supervisors on each site in accordance with Para 7 of the Model Rules and other ranks as per SLA.

#### 8.6.2.2 Eligibility Criteria

Eligibility criteria of the private security guards and supervisors shall be in accordance with the parameters given at Para 10 of The Act and those of other ranks shall as per SLA or PSA policy.

#### 8.6.2.3 Screening

Verification of character and antecedents of all personnel shall be in accordance with Para 4 of the Model Rules. Verification of the criminal record of the applicants shall be done on the Crime & Criminal Tracking Network & Systems (CCTNS) portal, where applicable.

#### 8.6.2.4 Health and Physical Fitness

The standard of physical fitness of private security guards and supervisors shall be determined in accordance with the parameters laid down in Para 6 of the Model Rules read in conjunction with the State Model Rules of the concerned State.

### 8.6.3 Employee Management

#### 8.6.3.1 Terms and Conditions of Employment

The Private Security Agency shall draft a comprehensive Standard Operating Procedure (SOP) with respect to the terms and conditions of their employees.

#### 8.6.3.2 Code of Conduct and Behavior

The PSA shall define a code of conduct for the security guards and supervisors and ensure that it is understood by all concerned. The code of conduct may include the following:

(a) Maintain personal discipline.
(b) Courteous behavior.
(c) Well turned out.
(d) Quick reaction to adverse situation.
(e) Salutation.
(f) Truthfulness.
(g) Alertness.
(h) Honesty.

#### 8.6.3.3 Disciplinary Code

The Agency shall define and document a Disciplinary Code in accordance with existing laws, for all its employees to follow. Some of the important breaches in discipline may constitute the following:

(a) Gross negligence in execution of duties.
(b) Failure to complete the assigned work in time.
(c) Misappropriation of funds entrusted for safe guarding.
(d) Committing/ abetting a cognizable offence.
(e) Deserting the place of duty without authority.
(f) Accepting bribes to allow unlawful activities.
(g) Consuming alcohol while on duty.

*NOTE This list is not exhaustive and does not necessarily include all actions.*

#### 8.6.3.4 Photo Identification

The Agency shall issue a photo-identity card to employed security guards and supervisors in accordance with PSARA Rules applicable, and for other ranks as per agency policy.

(a) the name, address and telephone number of the agency;
(b) the name of the employee, employee identification number and employee's signature;
(c) The photo-identity card shall clearly indicate the individual's position in the Agency and the date up to which the photo-identity card is valid. (not more than three years from the date of issue);
(d) A current full-face image colour photograph of the employee.
(e) The photo-identity card shall be maintained up to date and any change in the particulars shall be entered therein.
(f) Identity cards shall be formally withdrawn from employees when renewing their cards or leaving the organization, and destroyed in a secure manner.
(g) Any loss or theft of photo-identity card shall be immediately brought to the notice of the Agency.
(h) Maintenance of register for issuance and withdrawal and termination for all employees to be maintained.

This record shall also indicate the status and location of withdrawn cards, e.g. whether they have been destroyed or lost, or where they are held by the employee/organization.

#### 8.6.3.5 Records of Employed Staff

The agency shall maintain records with following details for all security guards and supervisors and other ranks of the Private Security Agency.

(a) Name of the guard, supervisor and other ranks
(b) Father'sname
(c) Present and Permanent address
(d) Phone numbers
(e) Nationality
(f) Date of joining/leaving the agency
(g) Photograph
(h) Badge/ Token/ Employee No.
(i) Salary with date
(j) Any other relevant details

### 8.7 Equipment and uniforms

### 8.7.1 Uniform

**8.7.1.1** Guards and supervisors shall be supplied with a uniform to wear when on duty as per applicable PSARA rules in order to ensure smart turn out of the guards and supervisors. The uniform should not resemble those of Armed Forces, CISF or other Government agencies. Where specified under SLA by the customer, the agency may change the colour and design as permissible, but shall ensure clear display of the insignia of the agency.

**8.7.1.2 Seasonal Uniform**

The agency shall ensure applicable seasonal uniforms are issued to its guards and supervisors and other ranks.

**8.7.1.3 Emergency and safety Equipment**

Some clothing, such as a high visibility (florescent) jackets, belts, helmets, safety shoes, masks etc, shall be issued to duty personnel as per site instructions and/or applicable safety rules.

**8.7.1.4 Ceremonial and Event Equipment and Uniform.**

Ceremonial and Event Equipment and Uniform shall be issued as per site requirements.

**8.7.1.5.Training Equipment and Uniform**.

The agencies conducting training shall ensure the required equipment and uniform are in use by the trainees.

### 8.7.2 Other equipment

All equipment used by guards and supervisors or provided as per SLA to a customer shall be appropriate for the intended use, in good working order and maintained regularly.

### 8.7.3 Vehicles

Operational vehicles, if held shall clearly display the organization's name, badge or logo, and telephone number in accordance with MV Act. Operational vehicles shall:

(a) be appropriate for the intended use;
(b) carry a two-way communication device;
(c) be inspected by the organization at least once per month to ensure that they are roadworthy;
(d) be serviced regularly, in accordance with the manufacturer's instructions;
(e) have any damage repaired as soon as possible;
(f) Be kept clean and tidy.
(g) Conform with all applicable rules and regulations.

Records of vehicle maintenance and repair shall be maintained.

### 8.7.4 Uniform and Equipment records

Records shall be kept of all uniform and equipment issued as per applicable SOP of the agency. Agency shall require employees to sign for equipment and uniforms received, and to give an undertaking to return equipment on termination of used.

## 9 Performance Evaluation

### 9.1 Monitoring, measurement, analysis and evaluation

**Level 1:** The PSA shall monitor, measure and regularly evaluate compliance with applicable legal obligations as identified in 4.5. The organization shall keep records of the results of the periodic evaluations.

**Level 3:**

#### 9.1.1 Site Performance Evaluation

Each static site shall have a written plan for regular supervisory/management visits. A qualified person who is independent of the running of that static site shall undertake the visits that should include checks on:

(a) The validity of the assignment instructions;
(b) The satisfactory maintenance of records

Periodic review meetings as mutually decided shall be held with the customer to discuss performance against both, the terms of contract and the assignment instructions. During such meetings any incidents which might have occurred shall be discussed, reviewed and further action to be taken shall be evolved. The records of monitoring undertaken from time to time shall be made available at the time of review for information of the customer.

Copies of the minutes shall be retained on the customer file as well as the agency files.

#### 9.1.2 Appraisals

Performance appraisal of the lower security functionaries by the senior functionaries shall be undertaken and recorded. The appraisal should include skills with reference to training, maintenance of documents, potential areas of improvement and key area performances.

#### 9.1.3 Complaints and grievances

The agency shall establish a complaints management system and define procedures to receive and resolve complaints from customers and other stakeholders.

The agency shall nominate a Nodal Officer/ single point of contact, for the purpose. The name and contact details of the Nodal Officer shall be communicated to all concerned. The Nodal Officer shall maintain a Complaint Register which shall be updated regularly.

#### 9.1.4 Feedback

The agency shall have an established procedure for obtaining feedback from a cross section of its customers on a regular basis. The feed backs shall be analyzed and corrective actions, if any, shall be taken.

**Level 5:** The requirements specified in 9.1 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 9.1 of ISO 18788:2015 applies.

### 9.2 Internal Audit

**Level 1:** The PSA shall conduct audits at planned intervals in order to determine whether or not the compliance practices and procedures:

a) conforms to:

1) the organization's own planned arrangements for achieving compliance with applicable statutory and regulatory requirements;

2) the recommendations of this Technical Criteria and relevant legal requirements;

b) is effectively implemented and maintained.

Additional audits can also be conducted as required.

The PSA shall:

- plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) should take into consideration the importance of the processes concerned and the results of previous audits;
- define the audit criteria and scope for each audit;
- select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
- ensure that the results of the audits are reported to relevant management;
- take appropriate correction and corrective actions;
- retain documented information as evidence of the implementation of the audit programme and the audit results.

**Level 3:** The PSA shall conduct audits at planned intervals in order to determine whether the private security services management system:

a) conforms to:

1) the organization's own requirements for private security services management system;

2) the recommendations of this Technical Criteria and relevant legal requirements;

b) is effectively implemented and maintained.

**Level 5:** The requirements specified in 9.2 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 9.2 of ISO 18788:2015 applies.

### 9.3 Management Review

**Level 1:** Top management shall review the PSA's compliance system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The actual depth and frequency of such reviews will vary with the nature of the organization and its policies.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) the adequacy of the compliance policy;

c) the extent to which the compliance objectives have been met;
d) adequacy of resources;
e) changes in external and internal issues that are relevant for compliance;
f) information on the compliance performance, including trends in:
- nonconformities, corrective actions and timelines for resolution;
- monitoring and measurement results,
- communication from interested parties, including complaints;
- audit results;

g) opportunities for continual improvement.

The outputs from management reviews shall include decisions and actions related to possible changes to the policies and procedures for compliance with applicable statutory and regulatory requirements and where possible continual improvement.

**Level 3:** Top management shall review the organization's private security services management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review shall be planned and carried out taking into consideration:
a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the quality management system;
c) information on the performance and effectiveness of the private security services management system, including trends in:
1) customer satisfaction and feedback from relevant interested parties;
2) the extent to which PSSMS objectives have been met;
3) process performance and conformity of products and services;
4) nonconformities and corrective actions;
5) monitoring and measurement results;
6) audit results;
7) the performance of external providers;

d) the adequacy of resources;
e) opportunities for improvement.

The outputs of the management review shall include decisions and actions related to:
a) opportunities for improvement;
b) any need for changes to the private security services management system;
c) resource needs.

The organization shall retain documented information as evidence of the results of management reviews.

*Note: The information on the performance relates both to the effectiveness in achieving intended objectives and the efficiency of procedures and processes. Measures of organizational performance may include customer satisfaction, service quality, productivity and growth.*

**Level 5:** The requirements specified in 9.3 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 9.3 of ISO 18788:2015 applies.

## 10 Improvements

### 10.1 Nonconformity and corrective action

**Level 1:** The PSA shall take immediate action to correct the observed non-conformance and then take further action to eliminate causes for any non-conformity and potential causes in order to prevent occurrence and recurrence respectively.

Any corrective and preventive action taken to eliminate the causes of actual and potential non-conformances shall be appropriate to the magnitude of problems encountered.

Records of action taken and improvements effected shall be maintained. The organization shall report non-compliance with any legal requirement to the concerned regulatory authority as required under the applicable legal requirements.

**Level 5:** The requirements specified in 10.1 and 10.2 of ISO/IEC 9001:2015 applies.

**Level 7:** The requirements specified in 10.1 of ISO 18788:2015 applies.

### 10.2 Continual Improvement

**Level 1:** The PSA shall seek to continually improve the suitability, adequacy and effectiveness of the compliance practices and procedures for achieving compliance with applicable statutory and regulatory requirements.

The information collected, analysed and evaluated accordingly, and included in compliance reports, shall be used as basis to identify opportunities for improvement of compliance performance of the organization.

**Level 3:** The PSA shall continually improve the suitability, adequacy and effectiveness of the private security services management system.

The PSA shall consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities that shall be addressed as part of continual improvement.

**Level 5:** The requirements specified in 10.3 of ISO/IEC 9001:2015 applies.

*Note: The PSA may consider Benchmarking of organizational performance using best practices from reference models, competitors and industry leaders in order to identify opportunities for improvement.*

**Level 7:** The requirements specified in 10.2 of ISO 18788:2015 applies.