An tÚdarás Slándála Príobháidí
The Private Security Authority

The Security Regulator

Public Consultation

Requirements for Access Control Contractors in the Private Security Industry.

Summary of Public Consultation	
Agency: Private Security Authority	**Legislation:** The Private Security Services Acts 2004 and 2011
Subject: Electronic Security-Access Control	**Date:** 12th November 2018
Related publications: Public Consultation 29th May 2017	
Contacts for enquiries: Ian Murray : 062-32659 Josephine Crowe: 062-32616	**Email:** public_consultation@psa.gov.ie

Agency and Legislation

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

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

Why is this Public Consultation being issued?

The PSA currently licence contractors who install Electronic Security-Access Control. As part of the licensing criteria, the PSA wishes to prescribe the requirements which contractors must meet and adhere to. The PSA has already held a public consultation in this area in 2017, however significant changes have been made to this document, in particular the removal of Powered Gates as this will be addressed in a separate document, and the division of management requirements into a separate document PSA 74:2018 which is also part of this consultation.

The security industry and the public expect all those working in the industry to provide an effective security service without posing any undue risk to the public. The PSA believes that the Requirements Document set out in this consultation will contribute to meeting this expectation.

PSA Requirements for Installers of Access Control

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

Responding to this Public Consultation

This Public Consultation is being issued for the information of contractors, industry stakeholders, interested parties and the public. Comments on same should be made to the PSA by the 7th January, 2019.

By email at: public_consultation@psa.gov.ie

or

By post to:

The Private Security Authority
Davis Street
Tipperary Town
Co Tipperary
E34 PY91

The closing date for receipt of comments is Monday 7th January, 2019.

An tÚdarás Slándála Príobháidí
The Private Security Authority

The Security Regulator

PUBLIC CONSULTATION DOCUMENT

PSA LICENSING REQUIREMENTS

Electronic Security - Access Control

(PSA 67:2018)

Standard For The Licensing Of

Access Control Contractors

November 2018

www.psa.gov.ie

Contents

1. SCOPE

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

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

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

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

- Specifying qualifications or requirements for the granting of licences.

Contractors licensed by the Private Security Authority and those seeking a licence from the PSA must comply with this standard. Only certification bodies approved by the PSA may provide certification services for licensing purposes. Contractors should check the PSA website, www.psa.gov.ie, for a list of approved certification bodies.

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

This document is for the purpose of licensing by the PSA and should not be interpreted as meeting any other statutory obligations of a contractor. It is not a technical reference. Contractors seeking a licence in the Access Control sector must also comply with the PSA Licensing Requirements for Security Service Providers (PSA74:2018).

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.

Acknowledgement: The PSA would like to acknowledge the contribution of all those who participated in the development of this document and to thank the National Security Inspectorate (NSI) who provided us with permission to reproduce in full and part extracts from their Code of Practice (NCP109.2)

2. DEFINITIONS

2.1 **Access Control.** The control or recording of access by persons or vehicles to or within premises by means of:

a) Personal identity verification, including by means of biometrics
b) Vehicle identification
c) Numerical codes
d) Alphabetical codes
e) Access or other card management,
f) Electronic key management, or

any combination of such means.

2.2 **Access point.** The position at which access can be controlled by a door, turnstile or other secure barrier.

2.3 **ACU.** Access control unit, or device which processes data from the reader to authorise or reject access.

2.4 **Approved Certification Body.** A certification body approved by the PSA to provide certification services in respect of Access Control.

2.5 **Biometric.** A measureable, unique physiological characteristic or personal trait that is used as a credential.

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

2.7 **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.

2.8 **Controlled Area.** The area to which access is permitted through the presentation of a valid credential.

2.9 **Credential.** Any token or memorised information or biometric used to identify an individual to an access control system in order to verify user access.

2.10 **Data bus.** A system within a computer or device, consisting of a connector or set of wires, that provides transportation for data.

2.11 **Fail locked.** The securing of a locking mechanism at an access point in the event of identified system failures.

2.12 **Fail unlocked.** The release of a locking mechanism at an access point in the event of identified system failures.

2.13 **Organisation**. A limited or unlimited company, a partnership or sole trader providing services installing, maintaining, repairing or servicing electronic security equipment, for which a PSA installer of security equipment (Access Control) licence is required.

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

2.15 **Reader.** Equipment for the extraction of data from a token or reader.

2.16 **Security Service.** The provision of access control services for which a PSA licence is required.

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

2.18 **Token.** A device such as an electronic key or card which is assigned to a user and which generates an authentication code which allows access.

3. GRADING OF ACCESS POINTS

3.1 Access points are graded by the requirements for successful legitimate access (see Grade I, Grade II, Grade III and Grade IV below). Grading is related to the level of security provided for each access point and the grade may change according to the time of day or night.

3.2 For each grade, access may be granted by the use of credentials permitted at higher grades, but not by the use of credentials permitted at lower grades.

3.3 Organisations shall determine the grading of each access point during the design stage, this shall be done in conjunction with the client and should be sufficient for the client's requirements.

3.4 Organisations shall include the location and grading of each of the access points making up an access control system in the system design proposal and in the as-fitted document.

a) Grade I (low risk)
At an access point to grade I, access will only be granted following:

- The input of a correct common code (or the input of a correct PIN code) of not less than 10,000 differs.
- 10,000 differs requires a 4 digit code number such as 1234.

b) Grade II (low to medium risk)
At an access point to grade II, access will only be granted following:

- Option A - the input of a correct PIN code of not less than 1,000,000 differs; or
- Option B - the presentation of a valid unique token to a reader.
- 1,000,000 differs requires a 6 digit code number such as 123456.

c) Grade III (medium to high risk)
At an access point to grade III, access will only be granted following:

- Option A - the input of a correct PIN code of not less than 10,000 differs AND the presentation of a valid unique token to a reader, or
- Option B - the presentation of a valid biometric to a reader.

d) Grade IV (high risk)
At an access point to grade IV, access will only be granted following:

- Option A - the presentation of a valid biometric to a reader AND the presentation of a valid unique token using radio frequency identification (RFID)*, comparative alternatives or
- Option B - the presentation of a valid biometric to a reader AND the presentation of a valid unique token to a reader AND the presentation of a correct PIN code of not less than 10,000 differs.

* RFID shall not rely on recognising the Chip Serial Number (CSN) only. Also the code to be read shall be stored in the memory of the card.

4. LOCATION SURVEY

4.1 Where relevant, organisations shall consult with relevant managers such as those responsible for information technology and human resources at the customer's premises.

4.2 In carrying out a location survey the following elements shall be fully taken into account:

a) The degree of physical security and the anticipated number of users and the duty cycle of the access point to which they are fixed;

b) Environmental factors, particularly when planning to use mechanisms externally:

- temperature
- humidity
- corrosion
- vibration
- dust and other contamination
- physical abuse

c) The degree to which external factors will affect the level of security required such as:

- the existing physical strength of the access point, such as doors and frames.
- the transfer of electrical connections onto doors shall be via suitable flexible cables or other means of adequate reliability.
- appropriate hardware shall be used where rebated and double-rebate doors are controlled.
- necessary safety precautions shall be taken where all-glass or other special doors are controlled.
- door closing devices shall be sufficient to close and lock the door under normal circumstances, but without undue impact upon the components of an access control system.
  Where adverse air pressure exists, organisations should provide means for relief of the air pressure.
- doors shall be a satisfactory fit in the frame.
- hinges, frame and fixings shall be adequate for the weight and proposed usage of a door.
  Organisations should follow manufacturers' recommendations for turnstiles and similar barriers, and their release mechanisms.
- where manual or automatic override features are used, continuously rated releases will be required.
  Access point hardware alone may not provide sufficient physical security in some circumstances.

The degree of physical security is related to the grading of access points. An access point to a higher grade will usually require greater physical security than an access point of a lower grade.

Organisations should select the necessary locking mechanisms to be appropriate to the strength of the door and its frame which should not reduce the physical strength of the access point significantly when fitting the mechanisms.

5. SYSTEM DESIGN

Access point design has a substantial bearing on the performance and reliability of an access control system.

5.1 Access points shall not:

- conflict with fire regulations
- restrict exit in such a way as to endanger people in an emergency.

5.2 Organisations shall consider the following aspects when designing an access control system:

- how access points will operate in the event of mains power failure and the period, or number of transactions, required in such circumstances;
- whether access points should fail locked or fail unlocked;
- whether secondary non-controlled locking devices should be fitted on external doors that fail unlocked;
- whether a key override is required for any critical doors to facilitate access in an emergency;
- whether ACUs will retain data in the event of data bus or power failure until the central computer or processor is operational;
- whether standby power is needed for the database (for example if held on a computer) to maintain its integrity during power failure;
- the choice of access control technology to provide an appropriate level of security for the risk to be protected;
- the choice of electronic equipment and its siting, taking into account environmental conditions and the potential for vandalism;
- the selection of access point hardware, taking into account the volume of traffic, environmental conditions and the level of physical security required;
- the number of users, access levels and time zones required, taking into account both present and predicted numbers of users and their needs;
- whether certain equipment needs to be protected against malicious damage;
- the need to site equipment such as controllers and printers in a secure area;
- the number of access points required, taking into account peak periods of use;
- whether an existing customer local area network (LAN) should be used;
- ease of access to ACUs and power supplies for preventative and corrective maintenance.

6. EQUIPMENT SELECTION AND INSTALLATION

6.1 Except where otherwise specified, equipment shall be selected and installed to withstand the following air temperatures:

- Internally sited equipment, 0 ºC to +40 ºC
- Externally sited equipment, -20 ºC to +50 ºC

6.2 Equipment exposed to direct sunlight can exceed these temperatures and appropriate shielding may be required in such circumstances. When the temperature is not well maintained internally in premises, temperature may vary between -10 ºC to +40 ºC and organisations should consider using equipment suitable for external use or similar. In all cases equipment should be suitable for use in the environment in which it is installed.

6.3 Organisations shall use environmental housings according to EN 60529 so as to afford appropriate protection (for example to IP54 or IP65 as applicable) where the possibility of penetration by solid objects, dust or water exists.

6.4 **Credentials**

Credentials may be thought of in terms of:

- something you know (code),
- something you have (token) or
- something you are (biometric).

6.4.1 The security, size and durability of a credential are dependent upon the technology used to encode it and the equipment required to read it.

6.4.2 Credential technology should be selected as appropriate to the risk being considered and the needs of the customer.

6.4.3 Several types of credential are available including:

a) memorized information such as common codes and PIN codes, which are input by hand to a keypad;
b) magnetic token, including Wiegand effect;
Where magnetic tokens are powerful enough to corrupt other magnetically stored data in their immediate vicinity they should carry a printed warning to this effect.
c) infra-red token;
d) hologram token;
e) proximity tokens using technologies such as radio or induction to allow the encoded data to be read within a specified operating range;
f) biometric.

When selecting a battery powered active token the life span of the battery and the environment in which the token will be required to operate and the frequency of its use shall be taken into account.

6.5 **Readers**

6.5.1 Readers shall be mounted:

- securely in position.
- adjacent to their access points and in positions convenient for all users to use, including those with disabilities.

6.5.2 Organisations shall provide a reader or controller and/or its associated access point hardware or a central control with the following features:

- an indication for access granted.
- variable time available for access to be made.
- tamper detection to detect access to the lock in circumstances where the lock can then be controlled from the insecure side.
- response within 2 seconds of the valid completion of the necessary data entry associated with the credential.
  Processing of more complex data such as those associated with biometric credentials may take longer than 2 seconds and this is acceptable provided the length of time is appropriate to the needs of the customer.
- re-locking of an access point if it is not used within a predetermined time.

6.5.3 When biometrics are used, the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) should be balanced to reflect the need for security on the one hand and the need for operability on the other hand. If the FAR is high then it will be more likely that an unauthorised person will be able to gain access using their biometric. Accordingly, customers should not normally be provided with the means to adjust biometric readers as this could seriously weaken the security of the access control system.

6.5.4 If the customer is provided with means to adjust biometric readers then access to the means of adjustment shall be protected against unauthorised change (for example by requiring an authorised person/manager to enter a password) and the customer shall be provided with sufficient information to enable them to understand the consequences of making adjustments. For example, the customer might be provided with information about the adjustments of their biometric readers that are acceptable and/or unacceptable for their security application.

6.6 **Access point hardware**

6.6.1 Organisations shall select access point hardware:

a) In accordance with the degree of physical security and the anticipated number of users and the duty cycle of the access point to which they are fixed;

b) With regard to the following, particularly when planning to use mechanisms externally:

- temperature
- humidity
- corrosion
- vibration
- dust and other contamination
- physical abuse

c) Taking into account the following with regard to the nature of the access point:

- the existing physical strength of the access point, such as doors and frames.
- the transfer of electrical connections onto doors shall use suitable flexible cables or other means of adequate reliability.
- appropriate hardware shall be used where rebated and double-rebate doors are controlled.
- necessary safety precautions shall be taken where all-glass or other special doors are controlled.
- door closing devices shall be sufficient to close and lock the door under normal circumstances, but without undue impact upon the components of an access control system.
  Where adverse air pressure exists, a means for relief of the air pressure should be provided.
- doors shall be a satisfactory fit in the frame.
- hinges, frame and fixings shall be adequate for the weight and proposed usage of a door.

d) Organisations shall follow manufacturers' recommendations for turnstiles and similar barriers, and their release mechanisms.

- where manual or automatic override features are used, continuously rated releases will be required.

6.6.2 Access point hardware alone may not provide sufficient physical security in some circumstances.

6.6.3 The degree of physical security is related to the classification of access points. An access point to a higher grade will usually require greater physical security than an access point of a lower grade.

6.6.4 Organisations should select the necessary locking mechanisms appropriate to the strength of the door and its frame and should not reduce the physical strength of the access point significantly when fitting the mechanisms.

6.6.5 The physical strength of an access point should be reinforced if this is likely to be unduly reduced by the attachment of the access control hardware. If this is not possible for any reason, the facts of the situation shall be provided in writing to the customer.

6.6.6 Where access point monitoring is of critical importance, consideration should be given to monitoring the locked / unlocked state of the access point, in addition to any monitoring by means of a separate protective switch.

6.6.7 Locking mechanisms can have two modes of operation under system failure conditions, 'failed unlocked' and 'fail locked'. Where exit is available by purely mechanical means, the fail locked mode may be acceptable but where exit is granted by electrical means, the 'fail unlocked' mode may be mandatory to meet safety legislation.

6.6.8 In the case of a complete power failure it may be necessary to provide a key override to a critical door (or doors) with the key (or keys) kept in a safe place outside the controlled door (or doors).

6.6.9 The suitability of any access control system shall be considered in relation to the fire risk assessment for the premises and the need for safe exit in emergency situations.

6.6.10 Where applicable, agreement shall be reached on what methods are to be used to release all the access points (for example green coloured single action emergency exit buttons, or break glass units, on the secure sides of access points) and these methods shall be documented in the system design proposal and the as-fitted document.

6.7 Power supplies

6.7.1 Organisations shall ensure the power supply to meet the largest load likely to be placed upon it under normal operational conditions is selected.

6.7.2 All equipment housings shall be clearly marked with the operating, or supplied, voltage. Where ACUs use external power supplies, ACU input voltages should not exceed 50V or 75VDC unless unauthorized access to both power supply and ACU are prevented.

6.7.3 Certain release mechanisms associated with an access control system, such as those for roller shutters, may operate at mains voltage and specific electrical safety requirements will apply to these.

6.7.4 Where safety and security considerations do not require continued operation of a system during a mains supply failure, the public mains supply via a safety isolating transformer may be the sole supply for the system. A 'clean' source for this may be required in electrically noisy environments.

6.7.5 Organisations shall:

- locate power supply units within controlled areas and in positions secure from tampering;
- consider additional security for power supply units that incorporate fail unlock hardware;
- connect the mains power supply permanently to the access control system via a fused outlet, not by plug and socket;
- not bring extra low voltage cables into a power supply container through the same entry point as any mains cables (except where impractical to avoid doing so).

6.7.6 Where continued operation of the access control system is essential during mains supply failure, a standby power supply shall be used having the necessary capacity to support the system for not less than the minimum period as agreed with the customer.

6.8 Cables

6.8.1 Where practicable, cables shall be installed within controlled areas.

6.8.2 Where practicable, cables shall be concealed.

6.8.3 Where cables are exposed to possible mechanical damage or tampering, or are outside controlled areas, they shall be protected by suitable conduit, trunking, or armour.

6.8.4 Where an access point release signal passes outside of a controlled area, metal conduit (or equivalent protection) shall be used.

6.8.5 All interconnecting wiring shall be supported and its installation shall conform to good working practice.

6.8.6 All extra low voltage cable joints shall be made in suitable junction boxes using either soldered, crimped, or screw-terminals. Alternatively plugs and sockets can be used provided fire safety is not compromised.

6.8.7 Extra low voltage signal cables shall not run in close proximity to mains power cables or other low or high voltage cables.

6.8.8 Signal cables for the transmission of data or other low level signals shall be of a type and size compatible with the rate of data transfer and anticipated levels of electromagnetic interference.

6.8.9 Low voltage cables from both mains and standby power supplies to remote equipment shall be of sufficient rating to permit satisfactory operation of the equipment at the end of any proposed length of cable run.

6.9 Control

6.9.1 Organisations shall consider the following when selecting controls:

- operational requirements of the associated controllers;
- protection against unauthorised interference with the system database or programme;
- logging of transactions;
- annunciation of alarms;
- blocking, validation and deletion of tokens;
- database for the retention of token holder details with back-up copies of corruptible data to facilitate re-establishment of the system in the event of a failure;
- programming of access levels and time zones;
- period of operation following mains failure and/or storage of data by non-volatile means;
- ease of access for maintenance and serviceability.

6.9.2 Organisations shall take into consideration the following when siting control equipment:

- ventilation;
- access for maintenance;
- user access for archiving;
- physical security and supervision;
- general visibility to unauthorized people of any displayed data.

7. INSTALLATION AND MAINTENANCE

7.1 Organisations must check the following during commissioning:

- all wiring is correctly terminated;
- alignment and operation of access point hardware and of release and closure mechanisms at each access point is correct;
- emergency release mechanisms at all the access points are in full working order;
- operation of each reader is correct;
- release time for each door is correct;
- door held open signal, if specified, is present;
- correct authorisation of access is verified by the input of appropriate data;
- access control system continues to work when mains supply disconnected (if specified).

7.2 At handover, organisations must:

- provide a system log book to the customer and explain how to record/report problems;
- demonstrate all aspects of the system operation to the customer, including any necessary safety precautions and any standby power facilities;
- ensure that the correct documentation is given to the customer to enable the system to be operated, adjusted and maintained;
- train the users in the correct operation of the system and arrange for any further training if necessary;
- for PC based systems, train the users on how to produce a system back-up and recommend that back-ups are carried out on a regular basis.
- ensure that users know the procedure for summoning assistance in the event of system malfunction;
- advise the customer to establish whether personal information held within the system requires registration under the Data Protection Act.

Where an access control system is managed remotely, details of this should be included in the documentation, for example the method of control and where control is carried out.

7.3 Maintenance

7.3.1 Where an organisation enters into a maintenance contract with a client it shall be documented and shall specify the schedule of maintenance agreed.

7.3.2 During each maintenance visit, inspection of the following, with all necessary tests, and those rectifications which are practical at the time, must be carried out:

(a) the installation, location and siting of all equipment and devices against the as-fitted document,
(b) the satisfactory operation of all equipment,
(c) all flexible connections,
(d) the normal and standby power supplies, for correct functioning,
(e) the control equipment,
(f) the operation of any warning device in the system,
(g) the correct operation of all system security functions,
(h) system application and operating software is at the correct version with any outstanding application and security patches and updates installed, subject to any software configuration controls the customer may have in place.

Repairs which were not carried out during the scheduled maintenance visit shall be completed as soon as is practicable, subject to the agreement of any charges which may be applicable.

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

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

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

7.3.6 A record of all maintenance visits and of the work carried out shall be maintained.

8. AS FITTED DOCUMENT

8.1 Upon completion of installation of the access control system an as-fitted document shall be produced including the following information:

- the name, address and telephone number of the controlled premises;
- the name, address and telephone number of the customer;
- the location and classification of each access point and the type and location of each controller and its associated hardware (for example the type of token/reader technology);
- the type and location of power supplies;
- power supply standby periods where relevant;
- details of those access points which the customer has the facility to override;
- the type and location of any warning device;
- details and settings of any preset or adjustable controls incorporated into the system;
- relevant documentation relating to equipment;
- relevant documentation relating to software functions;
- the number of keys, codes, tokens, and so on for the system provided to the customer;
- details of the methods adopted for emergency override for safe escape.

8.2 The as-fitted document shall be agreed with the customer and a copy provided to the customer.

8.3 Some of the information required for the as-fitted document may be provided in the form of a diagram of the installed system.

8.4 The customer should be advised to keep all documentation for the access control system in a place where access is restricted to authorized people.

8.5 For PC based access control systems, the software media may be handed over to the customer for safe keeping on site for use during service visits if required. A back-up of the initial system configuration (which may also include a copy of the database records) may also be handed over to the customer for system recovery if necessary.

9. COMPLIANCE WITH PSA LICENSING

9.1 Compliance With Standards

9.1.1 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.

9.1.2 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.

9.1.3 An audit report shall be completed by the approved certification body for each audit undertaken and the organisation shall agree to the certification body providing a copy of the report to the PSA.

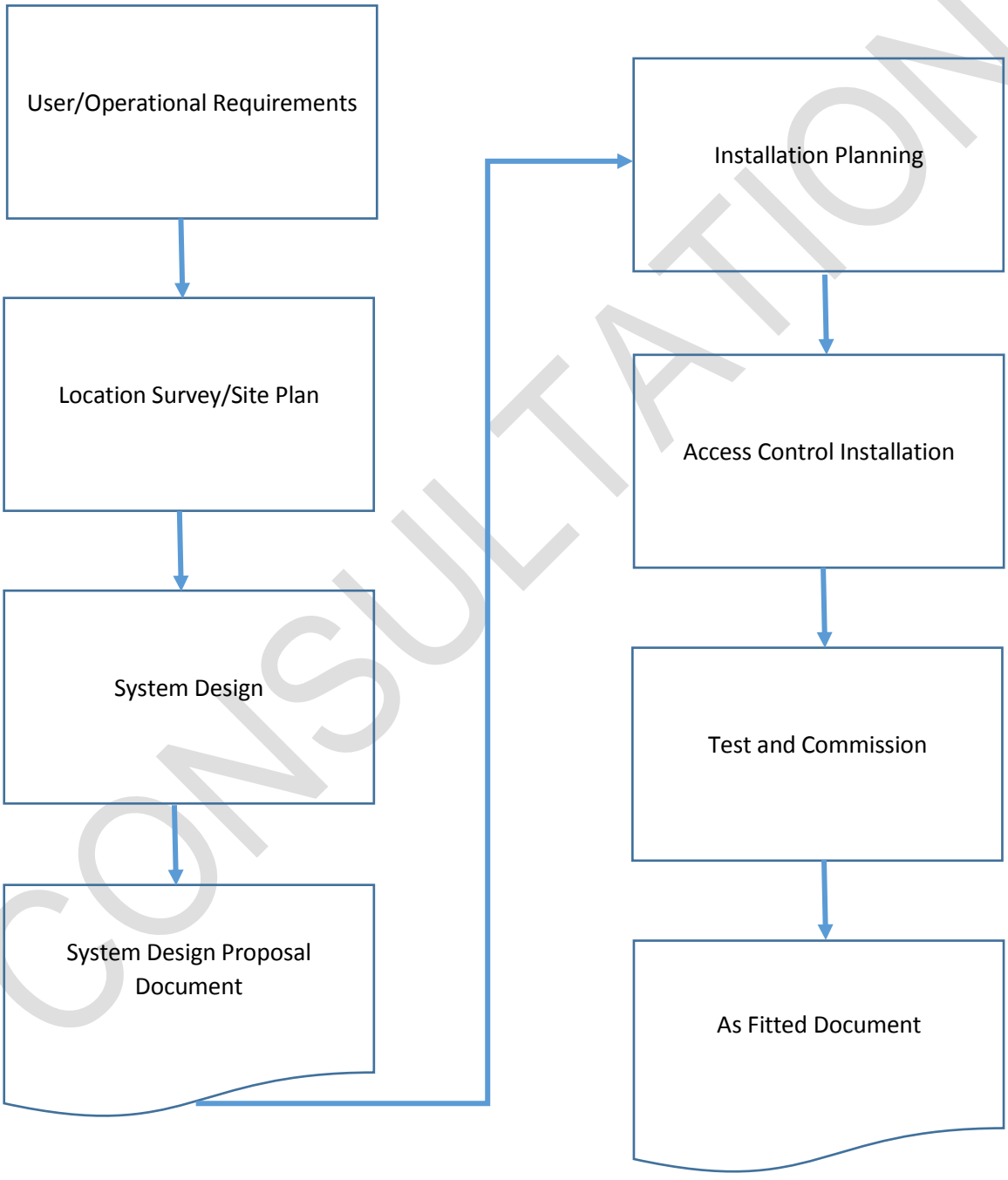
9.1.4 Organisations shall give their permission to the approved certification body to provide the PSA with information in accordance with provisions **7.1.5** and **7.1.6 of** PSA 74:2018 (PSA Licensing Requirements for Security Service Providers.

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

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

Annex 1

Flow Chart of Access Control Installations



Annex 2

Information to be included in the System Design Proposal

A system design proposal shall be prepared for the attention of the client or specifier (or his or her agent) of the Access Control system. The proposal shall include all the information necessary to enable the client or specifier to ensure the Access Control system is appropriate for the application. The information provided in the proposal shall include the following.

Client details
The name, address and the trading name (if different from the name of the client) and any other information necessary to clearly identify the client.

Contractor details
The name, address and trading name of the contractor (if a trading name is used) shall be included along with any other information necessary for the client to identify and/or contact the contractor. Headed company stationery with contractor details is acceptable in this regard.

Supervised area details
The name and address of the supervised area shall be included if different from the address of the client. This shall also include a description of the supervised area and an indication of what the area is used for.

Schedule of equipment
A schedule of the type and location of operational equipment (in words and/or diagrammatic form) shall be included.

Control
Details of the proposed control equipment shall be included.

Legislation
Details of any claims of compliance of the system components to any local or National legislation shall be included.

Standards
Details of any claims of compliance of the system components to any National or European Standards shall be included.

Annex 2(cont'd)

Other regulations
Details of any claims of compliance of systems components to any other regulations shall be included.

Certification
Details of any claims for certification of the system components shall be included.

Maintenance
The system design proposal shall include recommendations for the scheduled maintenance of the Access Control system or individual components including details of the frequency of any maintenance visits and a list of the work to be carried out during each visit.

When serviced the Access Control system shall be inspected, tested and adjusted to ensure correct operation in line with the functional requirements of the Access Control system as outlined in the As Fitted Document.

Care should be taken to ensure that the equipment is properly reinstated after testing. All maintenance shall be carried out in reference to the manufacturer's recommendations.

Repair
Details of the proposed repair service to be provided including contact names and telephone numbers.