

**MATTERS TO WHICH THE SECURITY AND GUARDING SERVICES
INDUSTRY AUTHORITY
SHALL HAVE REGARD WHEN DETERMINING
AN APPLICATION FOR A SECURITY COMPANY LICENCE**
(hereinafter referred to as ‘the Matters’)

Take notice that, pursuant to section 6(1)(b)(iii) of the Security and Guarding Services Ordinance, the Security and Guarding Services Industry Authority (hereafter referred to as ‘the Authority’) hereby specifies the following revised matters to which the Authority shall have regard when determining an application for a licence under the said Ordinance. This notice replaces the notice published as G.N. 630 in the *Government Gazette* on 28 January 2011, with effect from the day on which the notice is published in the *Gazette*. Different matters are specified in relation to different types of security work as follows: -

(I) Provision of Security Guarding Services

Company Background

- (a) The company must be a company registered in Hong Kong. The company will be required to produce the original and a copy of the Certificate of Incorporation as well as a Business Registration Certificate for the current year.
- (b) The company should have a sound financial background (see Note 1) and be able to furnish an appropriate financial reference from a Hong Kong bank or similar institutions.
- (c) The controller(s), the directors and executives are of good character, having regard to his/her criminal record and other relevant factors.
- (d) The company is appropriately insured for the extent of its business subject to a minimum of HK\$10 million per incident for public liability. Insurance should also include employee compensation. (See Note 2)

Premises

- (e) The company should have a place of business, the size, layout, and facilities of which is commensurate with its scale and nature of operations.

Control Room

- (f) The company, if required by nature of their work, should have a control room of adequate size which meets the following requirements:—
 - (i) Manned at all times during operating hours of the company.
 - (ii) The shell of the control room should be of substantial construction.
 - (iii) Doors of control room must be of minimum 40 mm solid core wood construction or equivalent.
 - (iv) Outer door(s) must be fitted with automatic self closing and locking devices.
 - (v) Access to the control room must be controlled by surveillance from within.
 - (vi) Access to the control room is restricted to authorised personnel only, (of which a movements log or an electronic data log capable of providing a printed copy on demand should be maintained inside the control room for a minimum period of 6 months).
 - (vii) Secure and adequate ventilation.
 - (viii) Standby lighting and power for uninterrupted operation and communications in the event of a mains failure for not less than 12 hours.
 - (ix) The fire service installations provided inside the control room must be maintained in efficient working order. Appropriate fire fighting equipment approved by the Fire Services Department is to be provided.
 - (x) If used for on-site alarm monitoring, a secure cabinet or safe for the protection of sensitive client

information should be provided with the following details recorded:—

- Name, address/unit and telephone number of the subscriber with an allocated reference number and details of any special arrangements or circumstances concerning the subscriber.
 - Name, address and telephone number of key holder(s).
 - Agreed setting/unsetting times.
 - All alarm events, for not less than 6 months (By printout on demand if stored electronically). The above data may be kept electronically provided that the data can be accessed by the inspecting officer upon request and the data is protected from unauthorised access and tampering, with proper back-up storage.
- (xi) An emergency duress alarm in the control room which when operated will directly summon assistance.
- (xii) The locking device should be operable without the use of a key from inside the control room or under the emergency entry procedure. The device should preferably not depend on any power supply.
- (xiii) A minimum communication requirement of one single direct telephone line.

Central Alarm Monitoring Station (CAMS)

- (g) The company when monitoring remote alarms off site, should have a CAMS which meets the following requirements:—
- (i) Manned 24 hours daily by a minimum of 2 persons.
 - (ii) The shell of the CAMS should be of substantial construction.
 - (iii) Doors of CAMS must be of minimum 40 mm solid core wood construction or equivalent.
 - (iv) Inner and outer doors should be fitted with automatic self closing and locking devices.
 - (v) Access by means of an ‘air lock’ system of interlocking doors.
 - (vi) Access to the CAMS must be controlled by surveillance from within.
 - (vii) Access to the CAMS is restricted to authorised personnel only, (of which a movements log or an electronic data log capable of providing a printed copy on demand should be maintained inside the CAMS for a minimum period of 6 months).
 - (viii) Secure and adequate ventilation.
 - (ix) Glazed areas kept to a minimum and of adequate construction.
 - (x) Standby lighting and power for uninterrupted operation and communications in the event of a mains failure for not less than 12 hours.
 - (xi) The fire service installations provided inside the CAMS must be maintained in efficient working order. Appropriate fire fighting equipment approved by the Fire Services Department is to be provided.
 - (xii) Secure cabinet or safe for the protection of sensitive client information with the following details recorded:—
 - Name, address and telephone number of the subscriber with an allocated reference number and details of any special arrangements or circumstances concerning the subscriber.
 - Name, address and telephone number of a minimum of 3 key holders.
 - The appropriate police area or security service to be contacted when an alarm occurs.
 - Agreed setting/unsetting times.
 - All alarm events, for not less than 6 months (By printout on demand if stored electronically).

The above data may be kept electronically provided that the data can be accessed by the inspecting officer upon request and the data is protected from unauthorised access and tampering, with proper back-up storage.
 - (xiii) Minimum of 2 telephones, with a minimum of 3 adequately protected lines (2 incoming and one hunting).
 - (xiv) Emergency exit doors, if any, with hinges, frames, fixings and unlocking devices constructed to offer resistance to entry following physical attack at least equivalent to that of a hardwood, 40 mm thick, faced on the outer surface with securely attached mild steel sheet, 1.5 mm thick.

- (xv) Emergency exit doors, if any, opening outwards, unless otherwise approved by the Security Companies Inspection Unit.
- (xvi) Emergency exit doors, if any, fitted with unlocking devices intended to be released only in event of an emergency.
- (xvii) The locking device should be operable without the use of a key from inside the CAMS or under the emergency entry procedure. The device should preferably not depend on any power supply.
- (xviii) Toilet and washing facilities should be provided within the CAMS, or if not, a duress code be fitted to an access control system.

Armoury

- (h) The Armoury should, if required, in all respects, fully comply with the requirements as laid down in the 'Firearms and Ammunition Ordinance, Chapter 238'.

Personnel

- (i) All personnel engaged in security work must have a valid permit.
- (j) The company must carry out its own employment vetting (see Note 3), which includes, where possible:—
 - (i) Employment history;
 - (ii) Reference check (referees should be non-relatives) or other acceptable modes of character check; and
 - (iii) Residential address check.

Training

- (k) The company must have a nominated training officer responsible for the training of all operational staff.
- (l) All training must be held in a suitable training facility (see Note 4).
- (m) Except when an employee produces a valid certificate issued to him in respect of a training course accepted by the Authority within 5 years, all employees, before performing operational duties, must undergo and pass an initial basic training course of not less than 16 hours, regardless of previous working experience, which includes:—
 - (i) Role, General Duties and Responsibilities of a Security Guard
 - (ii) Conduct and Behaviour
 - (iii) Uniform and Equipment
 - (iv) Legal Responsibilities and Relevant Legislation
 - (v) Fire Prevention and Procedures
 - (vi) Handling of Emergencies
 - (vii) Reporting and Recording
 - (viii) Access Control and Patrolling
 - (ix) Health and Safety
 - (x) Courtesy and Customer Relations
- (n) All employees deployed to operate a CAMS must undergo and pass relevant training in addition to the 16-hour initial basic training as prescribed in (I)(m) above before performing related operational duties. The duration and contents of the additional relevant training must comply with those prescribed in the "Course Profile of the Training for Central Alarm Monitoring Station Operators" as updated and announced from time to time by the Authority.
- (o) The results of these courses must be recorded in the employee personnel files.
- (p) A security company, which takes over another security company's business as well as its staff, may apply in writing to the Police with valid reasons for a grace period in providing initial basic training to its guards before performing operational duties.

Supervision

- (q) A company must maintain 2 full copies of assignment instructions for each duty post, (one in management records and one at the duty area), which should cover:—
- Name of the Employer
 - Address of the Duty Area
 - Telephone Procedures
 - Action in Emergencies
 - Fire Precautions
 - Crime Prevention
 - Guard Control Systems (Patrol Management System)
 - Guard Patrol Procedures
 - Access Control Procedures
 - Security System Operation Procedures
- (r) Unless the Commissioner of Police otherwise approves, a company must supervise all patrols on a shift basis through a minimum of one visit per week by the supervisor from an off-site location if teleprotection (see Note 5) is available, and one visit per shift if otherwise.
- (s) Occurrence Books must be maintained at every duty post.
- (t) All incidents must be recorded and investigated.

Disposal of Confidential Documents

- (u) Confidential documents no longer required must be shredded before being discarded.

Contingency Plans

- (v) The company should have contingency plans for fire and other disasters.

(II) Provision of Armoured Transportation Services*Company Background*

- (a) The company must be a company registered in Hong Kong. The company will be required to produce the original and a copy of the Certificate of Incorporation as well as a Business Registration Certificate for the current year.
- (b) The company should have a sound financial background (see Note 1) and be able to furnish an appropriate financial reference from a Hong Kong bank or similar institutions.
- (c) The controller(s), the directors and executives are of good character, having regard to his/her criminal record and other relevant factors.
- (d) The company is appropriately insured for the extent of the business that they pursue. Insurance should include employee compensation, public liability and cash fidelity insurance. The minimum amount for public liability is HK\$10 million per incident. (See Note 2)

Premises

- (e) The company should have a place of business, the size, layout, and facilities of which is commensurate with its scale and nature of operations.

Control Room

- (f) The company should have a specialised control room of adequate size which meets the following requirements:—
- (i) Manned by a minimum of 2 persons at all times during operating hours of the company.
 - (ii) The shell of the control room should be of substantial construction.
 - (iii) Doors of control room must be of minimum 40 mm solid core wood construction or equivalent.
 - (iv) Inner and outer doors should be fitted with automatic self closing and locking devices.
 - (v) Access by means of an 'air lock' system of interlocking doors.

- (vi) Access to the control room must be controlled by surveillance from within.
- (vii) Access to the control room is restricted to authorised personnel only, (of which a movements log or an electronic data log capable of providing a printed copy on demand should be maintained inside the control room for a minimum period of 6 months).
- (viii) Secure and adequate ventilation.
- (ix) Glazed areas kept to a minimum and of adequate construction.
- (x) Standby lighting and power for uninterrupted operation and communications in the event of a mains failure for not less than 12 hours.
- (xi) The fire service installations provided inside the control room must be maintained in efficient working order. Appropriate fire fighting equipment approved by the Fire Services Department is to be provided.
- (xii) Emergency exit doors, if any, with hinges, frames, fixings and unlocking devices constructed to offer resistance to entry following physical attack at least equivalent to that of a hardwood, 40 mm thick, faced on the outer surface with securely attached mild steel sheet, 1.5 mm thick.
- (xiii) Emergency exit doors, if any, opening outwards, unless otherwise approved by the Security Companies Inspection Unit.
- (xiv) Emergency exit doors, if any, fitted with unlocking devices intended to be released only in event of an emergency.
- (xv) The locking device should be operable without the use of a key from inside the control room or under the emergency entry procedure. The device should preferably not depend on any power supply.
- (xvi) Toilet and washing facilities should be provided within the control room, or if not, a duress code be fitted to an access control system.
- (xvii) A minimum communication requirement of one single direct telephone line.

Vaults and Vaulting Area

- (g) The vault and vaulting area should meet the following requirements:-
 - (i) Sterile loading/unloading facility for cash or valuables at the company premises.
 - (ii) Sterile loading/unloading area large enough to securely house at least one armoured vehicle.
 - (iii) The sterile area must be closed off at the vaulting side by a receiving hatch and by at least one roller shutter door (of a closed link structure) at the entrance.
 - (iv) The receiving hatch and entrance door should not be opened at the same time.
 - (v) The vault walls, floor and ceiling of a minimum 225 mm reinforced concrete construction or equivalent.
 - (vi) Vault doors of an adequate strength.
 - (vii) If not manned 24 hours the vault and vault area must have a monitored alarm with a direct connection to an approved central alarm monitoring station.
 - (viii) Walls of the vault perimeter area of a minimum 150 mm reinforced concrete block or equivalent.

Armoury

- (h) The armoury should, in all respects, fully comply with the requirements as laid down in the 'Firearms and Ammunition Ordinance, Chapter 238'.

Personnel

- (i) All personnel engaged in security work must have a valid permit.
- (j) The company must carry out its own employment vetting (see Note 3), which includes, where possible:—
 - (i) Employment history;
 - (ii) Reference check (referees should be non-relatives) or other acceptable modes of character check; and
 - (iii) Residential address check.

Training

- (k) The company must have a nominated training officer responsible for the training of all operational staff.
- (l) All training must be held in a suitable training facility (see Note 4).
- (m) All employees deployed as a member of an armoured vehicle crew must undergo and pass the relevant initial basic training for vehicle crew in addition to the 16-hour initial basic training as prescribed in (I)(m) above, regardless of their working experience. The duration and contents of the additional relevant training must comply with those prescribed in the “Course Profile of the Initial Basic Training for Vehicle Crew” as updated and announced from time to time by the Authority.
- (n) The results of these courses must be recorded in the employee personnel files.
- (o) All employees appointed as Vehicle Crew Commander and above must have satisfactorily completed and passed a suitable Crew Commander Training Course organised by the company’s training officer prior to the appointment. The duration and contents of the training must comply with those prescribed in the “Course Profile of the Training Course for Vehicle Crew Commanders” as updated and announced from time to time by the Authority.
- (p) A security company, which takes over another security company’s business as well as its staff, may apply in writing to the Police with valid reasons for a grace period in providing initial basic training to its guards before performing operational duties.

Security Transit Vehicle

- (q) The security transit vehicles of the company should meet the following requirements:—
 - (i) The cabs of the vehicles, including glazing materials must be ballistically resistant to a minimum 9 mm military handgun (parabellum).
 - (ii) The vehicle vault, if permanently manned, must be built to the same standard as the cab.
 - (iii) All vehicles must be fitted with a legal alarm for use in an emergency.
 - (iv) All vehicles must have an identification number painted on the roof of such a size as to be clearly visible from the air.
 - (v) All vehicles are fitted with a vehicle radio capable of communicating with the company cash control room at all times, on OFTA approved frequencies. Mobile phones can be accepted in lieu of a vehicle radio.
 - (vi) All vehicle windows are sealed and not open.
 - (vii) All vehicles are air-conditioned.
 - (viii) All vehicles are equipped with appropriate fire fighting equipment approved by the Fire Services Department.
 - (ix) All vehicles are manned at all times when transporting cash/valuables.
 - (x) All vehicles are insured, licensed and inspected in accordance with the Road Traffic Ordinance and subsidiary legislation made thereunder.

Disposal of Confidential Documents

- (r) Confidential documents no longer required must be shredded before being discarded.

Contingency Plans

- (s) The company should have contingency plans for fire and other disasters.

(III) Installation, Maintenance and/or Repairing of a Security Device and/or Designing (for any particular premises or place) a Security System Incorporating a Security Device

Company Background

- (a) The company must be a company registered in Hong Kong. The company will be required to produce the original and a copy of the Certificate of Incorporation as well as a Business Registration Certificate

for the current year.

- (b) The company should have a sound financial background (see Note 1) and be able to furnish an appropriate financial reference from a Hong Kong bank or similar institutions.
- (c) The controller(s), the directors and executives are of good character, having regard to his/her criminal record and other relevant factors.
- (d) The company is appropriately insured for the extent of its business subject to a minimum of HK\$10 million per incident for public liability. Insurance should also include employee compensation. (See Note 2)

Premises

- (e) The company should have a place of business, the size, layout, and facilities of which is commensurate with its scale and nature of operations.

Electronic Technical Workshop

- (f) The company should have an electronic and technical workshop of an adequate size, with sufficient facilities and test equipment to provide adequate service repair and equipment fabrication.

Test Equipment

- (g) The company should have sufficient test equipment and tools necessary for carrying out installation work, service repair and field services.
- (h) A detailed list of test equipment should be available at the workshop for record purpose.

Security Devices Requirements

- (i) All Security Devices designed, installed, maintained and repaired should be done according to the relevant British Standards (B.S.), European Standards, Underwriters Laboratories Inc. (U.L.) Standard or equivalent where appropriate and applicable.

Personnel

- (j) All personnel engaged in security work must have a valid permit.
- (k) The company must carry out its own employment vetting (see Note 3), which includes, where possible:—
 - (i) Employment history;
 - (ii) Reference check (referees should be non-relatives) or other acceptable modes of character check; and
 - (iii) Residential address check.
- (l) All staff carrying out alarm installation work and servicing must have adequate recognised technical qualifications or equivalent related experience.

Disposal of Confidential Documents

- (m) Confidential documents no longer required must be shredded before being discarded.

Contingency Plans

- (n) The company should have contingency plans for fire and other disasters.

Notes

(1) Sound financial background

In considering whether a company or a licensee has a 'sound financial background', the Police will examine the company's financial documents (e.g. bank reference letters, balance sheets, profits and loss accounts, financial guarantees from parent companies, etc.) in order to ascertain its financial

status. If the company/licensee is found to be in financial difficulties or suffering from significant financial losses, the company should account for the losses and explain to the satisfaction of the Police and the Authority how it would ensure sufficient working capital for the company's continuous operation, e.g. whether there would be any injection of capital from the shareholders, parent company or other sources.

(2) Insurance

- (a) A company or a licensee should take out insurance cover only with those regulated under the Insurance Companies Ordinance (Chapter 41).
- (b) The company should make available insurance certificates and premium receipts for Police inspection and notify the Police or Authority within 14 days in case of mid-term cancellation of policy.
- (c) Employees' compensation insurance cover should be procured in accordance with the Employees' Compensation Ordinance (Chapter 282).

(3) Employment Vetting

Before employing a security personnel, a security company must carry out its own 'employment vetting'. Such a vetting should cover :—

- (a) **verification of employment history** – requiring the person seeking to be employed as security personnel to provide information on his past employment including the name and contact details of past employers, position held and period of employment. The company should then verify this information through examining the authenticity of the certificates of employment or reference letters produced, and/or contacting the previous employers;
- (b) **conducting reference or character checks** – requiring the personnel to provide the name, address and telephone number of 2 persons as referees for the company to consult about his past performance, character and suitability to undertake security work. The reference may be provided to the company either in writing or verbally. A verbal reference should be properly recorded in the employee's personal file. Should the company have any difficulties in obtaining such reference, e.g. the referees cannot be located or are unwilling to co-operate, the company should put on record the steps taken to obtain the reference and the difficulties encountered. The Police would consider whether the absence of such reference is supported by good reasons and report the same in their subsequent investigation report to the Authority; and
- (c) **conducting residential address check** – requiring the personnel to provide his residential address and contact telephone number and produce supporting documents such as utility bills or tenancy agreement. The company should then verify this information through examining the authenticity of the documents produced and/or contacting the person at the given address or telephone number.

(4) Suitable training facility

A 'suitable training facility' should include:-

- (a) a room to conduct training, which is of a size enough to accommodate a minimum of 3 trainees;
- (b) training apparatus and equipment such as white/black boards, overhead projectors, flip charts and other types of teaching aids; and
- (c) training materials including training notes, syllabus and handouts that are relevant to the type of security services to be provided.

(5) Teleprotection

Definition

- (a) 'Teleprotection' means a supervisory system under which security guards are required to

make regular reports, by telephone or other equivalent means of communication, to their supervisors or control centres (if any) at designated times and frequency to ensure their personal safety and the well-being of the places under their responsibility.

Guidelines

Teleprotection by telephones

- (b) If teleprotection is available, the security guard at each guard post is required to make regular telephone reports to his supervisor or control centre, or vice versa, at fixed timing and frequency as follows:-
 - (i) *For the guard post manned by a single person*
 Day shift : At least once every 4 hours
 Night shift : At least once every 2 hours
 - (ii) *For the guard post manned by more than one person*
 Day shift or night shift : At least once every 4 hours
- (c) The company is required to stipulate the timing and frequency for such reports and record the same in the assignment instructions. All calls made and received must be properly recorded in a log-book at the receiving station.

Computerised teleprotection

Computerised teleprotection may only be carried out through a control room or a CAMS. Security companies shall show to the satisfaction of the Commissioner of Police that the following criteria are met: -

- (d) Verification of person – this may be accomplished by a variety of methods including, but not limited to, interactive voice response, ID swipe cards or biometrics.
- (e) Verification of location – this may be accomplished by caller number display on telephones or fixed location identification systems.
- (f) Verification of ‘No Duress’ – on logging in the interactive voice response system, voice call system or computer system, the security operatives should have options including, but not limited to, entering codeword and/or number, or pressing wrong input or using the wrong thumb, hand or eye for biometric systems, to indicate that they are under duress.
- (g) Capacity of the system – the system should have multiple access lines so that large numbers of operatives may log in at the same time; and the receiving system must be able to process multiple access simultaneously.
- (h) Failure response: -
 - (i) computer – the computer system should be so programmed such that an automatic computerised call back response is triggered for failures to login within a specified period of time after the scheduled log in; and/or
 - (ii) human – the computerised system should be so programmed such that should it fail to detect a missed log in, it should alert a human operative in the monitoring station of the situation.
- (i) Physical response (*times and actions*) – the human operatives will have to respond in accordance with a laid down contingency plan that stipulates the correct physical response required for each location, and the minimum response time required for completion.

- (j) The operations centre should be located in Hong Kong – this is essential in order for the Security Companies Inspection Unit to be able to fully assess the capabilities and security of the system to ensure that it meets the requirements of teleprotection.

Absence of teleprotection

- (k) In the absence of a teleprotection system, a company must supervise all patrols on a shift basis through a minimum of one visit per shift in line with item (I)(r) of ‘the Matters’.

Daniel Cham Ka Hung *Chairman, for and on behalf of the
Security and Guarding Services Industry Authority*

[The above was published in Government Gazette on 24 February 2012 (Government Notice No.: 953)]