Dated 28 Apr 20

**THE PROVISION OF A MANNED SECURITY GUARDING SERVICE AT PATHFINDER BUILDING - STATEMENT OF REQUIREMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.1  The guard force on duty is wholly responsible to the requirements of the Designated Officer in execution of their agreed tasks. | The command chain for the guard force is:  a. Head of Establishment  b. Establishment Security Officer  c. Pathfinder Security Manager - Designated Officer (DO)  c. DO authorised representative  d. Service provider’s Contract Manager  e. Service provider’s Guard Manager  f. Service provider’s Shift Supervisor | The Designated Officer is also referred to as the Authority within this document.  The DO representative is a member of the Security Section who has been authorised to deputise in his/her absence. |  |
| 1.2  Service provider shall be compliant with, registered or accredited as applicable.  1.3  Service provider to maintain 1.2 throughout the contract period. | 1. The Security Industry Authority (SIA) Approved Contractor   Scheme.   1. ISO 9001:2015 Quality Management and Quality Assurance   Standards.  c. BS 7499:2013 Code of Practice for Static Guarding, mobile  patrols and key-holding services. | These requirements are measurable within the KPI process. |  |
| 1.4  Service provider will be compliant with the Working Time Regulations 1998. (Amended 2007).  [EU’s Working Time Directive (2003/88/EC)](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32003L0088) | 1. Average 48-hour week over a nominal 17- week period. 2. EU WTD allows in certain circumstances, the 17- week   period to be extended to 52.  c. Shifts not to exceed 12 hours.  d. Maximum 56-hours in 7 consecutive days, must be given  48-hours consecutive time off.  e. Service provider to liaise with the DO for his approval in  exceptional circumstances if this cannot be met.  f. Service provider to factor in concentration times and regular  breaks for staff engaged in CCTV monitoring and demonstrate how this is being achieved.   1. Breaks (including reading materials) are to be taken away   from the workstation (no food is to be consumed within Security Posts and drinks are to be kept in a sealable container no less than 300mm away from console equipment)   1. All commitments are to be adequately covered. | These parameters are measurable within the KPI process. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.5  Service provider is to provide an adequate pool of employees who are security cleared to the required standards to ensure that the guarding requirements are met at all times. | 1. Pre-nominated and approved reserves are to be on 2 hours   notice to be on duty.  A minimum baseline manning ratio of Information Redacted .  The ratio of nominated reserves shall be Information Redacted for guarding tasks in this contract.   1. Continuity of cover must be provided for rest periods, tea &   meal breaks taken by guards or supervisors.   1. Approved reserves may be employed elsewhere within the   service provider’s company however, priority must be to the commitment of this contract if invoked by the DO.   1. The requirements of 1.4 shall apply to approved reserves   utilized on this contract even when not on this site.   1. Approved reserves may be called upon to cover short   notice sickness or absence.   1. Approved reserves can also be called upon with 5 working   days’ notice to provide cover for training as and when required by the DO. | These requirements and parameters are measurable within the KPI process.  Approved reserves are permitted to work on other sites; however, compliance with 1.4 will give a level of assurance that they are not fatigued prior to duty. |  |
| 1.6  Service provider to ensure all guard force personnel have been approved by the Designated Officer (DO) prior to the security clearance process. | The DO should be made aware of any known reason(s) that could potentially have an impact on an individual’s probability of being approved for DV Clearance | UKSV are the vetting authority who ultimately decide whether clearance is approved. |  |
| 1.7  Service provider to confirm in writing to the DO, either annually or on change of staff, that the guard or manager is medically fit for employment. | 1. If subsequently the guard or manager is found not to meet 2. 1.6 or 1.7, they should be withdrawn and replaced with an   approved substitute in the time specified in 1.5   1. Any medication which may have an adverse effect on the   guard’s ability to perform their duty, must be brought to the attention of the DO, the guard will be prohibited from being assigned to post.   1. Guards must not be colour-blind. | These requirements and parameters are measurable within the KPI process.  X-Ray scanners and other equipment present valuable graphical information for interpretation by colour variances. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.8  Staff Leaving | The service provider must inform the DO or his representative at the earliest opportunity that a staff member is leaving or has left, not to return under this contract. Staff must be de-inducted by the DO or authorised representative on site, travel outside of site to de-induct an individual, shall be at the cost of the service provider | Staff turnover is a measurable on the KPI. |  |
| 1.9  Service provider is to ensure guards complete and maintain the following training throughout the duration of the contract period. The Guard manager is to keep a documented training and development record for all guards. | 1. Security General Threat Brief (Annually) 2. Basic Fire Awareness (DLE\*) (Annually) 3. Display Screen Equipment (DLE\*) (every 2 years) 4. Equality and Diversity (CSL\*) (every 2 years) 5. Defence Information Passport (DLE\*) (every 3 years) 6. GPDR Course (DLE\*) (every 3 years) 7. Must have Data Protection Act awareness relating to,   Control Room practices.   1. Full operational effectiveness and skill share is an essential   part of this contract.   1. The service provider will be expected to demonstrate   compliance with requirement (1.9 h) by the operative achieving the following outline knowledge and competency levels:  Level 1 – Baseline  Level 2 – Operator  Level 3 – Practitioner  Level 4 – Expert  Level 5 – Supervisor | - Provided by the customer Security  -These requirements and parameters are measurable within the KPI process.  -The authority will deliver training within its scope.  -It is for the service provider to fund access to the Defence Learning Portal (DLE) in order to access online training.  -Guards will be trained on existing Security System elements including CCTV, Alarms and AACS and VMS |  |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.9  Service provider is to ensure guards and on-site supervisors have the following throughout the duration of the contract period.  CONTINUED… | j. Minimum requirement of Level 1:   * Visitor Management System- Guard Level Access * Execute external foot patrols * Compound duties – receipt of collections & deliveries * Escorting outside the building but within the fence line * Conduct Vehicle searching * Understand and apply search and finds procedure * Metal detection arch operation * Metal detecting wand operation * Mail intake process including suspect package identification and incident process * X-Ray machine basic familiarisation and image interpretation * Visitor process including clearances required, visitor warning lights, prohibited items. * Alarm response procedure * Two Way radio use and protocol * Phone detectors * Intercom operation * location and use of barriers and gates * Location of external plant and doors * External fire alarm points, hydrants, firefighting equipment and disabled refuge phone operation * Foyer reception duties * Identification of badges and lanyards and their rational     k. Minimum requirement of Level 2:   * Level 1 competencies attained * Floor plan layout and familiarisation * Location of all access-controlled doors * Location of all Intruder detection Points * Location of all fence zones * CCTV camera locations known | Intruder Detection System: Information Redacted  Intercom system: Information Redacted  Visitor Management System: Information Redacted  Security Management System: Information Redacted  X-Ray machines: Information Redacted  Phone Detection Systems: Information Redacted  Level 1. This list is not exhaustive; however, these are typical tasks which can be undertaken by an individual without the requisite clearance level to enter the SAO unescorted.  A person with Level 1 competency will not be allowed to work a shift pattern as the core skills do not meet with the SoR.  Level 2 onwards, will be suited to individuals who have the required clearance level for unescorted access within the building; the list is typical but not exhaustive.  These requirements and parameters are measurable within the KPI process. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.9  Service provider is to ensure guards and on-site supervisors have the following throughout the duration of the contract period.  CONTINUED…... | * Key control process understood * Daily Occurrence Book protocol * Receipt and Issue process * Internal fire alarm points and firefighting equipment * Emergency procedures * X-Ray competent in threat recognition * Reception duties – behind glazing * VMS badge production * Virus checking * Conduct counter compromise internal searches * Identify non-operational electrical equipment and switch it off   l. Minimum requirement of Level 3:   * Operation of automated access control system (AACS) –   locking/unlocking, interpret faults/warning messages   * Operation of the Security Management System (SMS) –   accept, reset, inhibit   * Operation of Intruder Detection System (IDS) – type of   sensors, principle of operation   * Operation of CCTV- control cameras/monitors, execute   virtual patrols   * Voice Alarm/ Public Address system * Radio base station operation * Fire alarm system procedure (under review)   m. Minimum requirement of Level 4:   * In depth knowledge of policies and procedures | The Levels and lists are indicative and not exhaustive, from the levels incremental knowledgebase builds ensuring that officers are sufficiently trained to deliver the full scope of the SoR to the satisfaction of the authority.  These requirements and parameters are measurable within the KPI process. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.9  Service provider is to ensure guards and on-site supervisors have the following throughout the duration of the contract period.  CONTINUED…. | n. Minimum requirement of Level 5:   * Retrieval of CCTV images of hard & soft copy * Auditing of all system information – AACS, IDS etc. * Trainer and performance responsibility   Time scales for achieving levels:  Level 1 – 3 months or less  Level 2 – 4 months or less  Level 3 – 5 months or less  Level 4 – 6 months or less  Level 5 – 4- 6 months  o. X-Ray Scanning equipment operation and object recognition  to be held by no less than 1 of the guards on duty throughout the  contract term.  p. All guards are to be First Aid trained and certified, this  certification must be current throughout the contract term.  q. Provide and maintain, CCTV DPA/Criminal Evidence  compliance kit, including coloured master disc and evidence  bags.  r. Guards and supervisors to be computer literate and have a working knowledge of Microsoft Word, Excel and Outlook. |  |  |
| Security Section to recommended enhancements above that required to provide minimum functionality and guard force effectiveness. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.10  Service provider to accommodate reasonable requests. | s. In an emergency or elevated Response Levels, the Designated Officer will have the right to order the service providers staff to perform such reasonable tasks as may be necessary for the security of the site. |  |  |
| 1.11  Service provider to supply suitable cleared personnel for the duration of the contract. | 1. The DO can authorise escorted access for the SC cleared   guard is escorted by a fully cleared person.   1. Full clearance is required for unescorted access within the   SAO, Security Control Centre, Main Security Post and the Secondary Security Post.   1. A fully cleared person holds Developed Vetting (DV) and is   fully inducted,   1. Guards are to read and sign as having understood   Pathfinder Security Orders.   1. Guards who fail the DV process or subsequently have   their DV status removed, will be deemed unsuitable to remain on site.   1. Any changes of circumstances which may affect an   individual’s clearance must be brought to the attention of the DO. | These requirements and parameters are measurable within the KPI process.  The authority will sponsor DV applications in the absence of the service provider being unable to provide this function. It should be noted that the authority will advise that the DV be cancelled should the individual no longer be used to cover this contract commitment. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.12  Service Provider to ensure minimal costs to the client contact mechanism. | Booking on calls, check calls and any other verbal or non-verbal communications from site to the service provider must be made to a standard charge land line and will be paid by the Authority throughout the duration of the contract. Calls to mobiles or premium rate numbers are not permitted. | The DO will receive a list of calls made on phones controlled by the service provider in Pathfinder. Any calls, other than booking on/off, particularly to mobiles or premium numbers are to be recorded in the DOB, with an explanation. Non work associated calls will be chargeable to the service provider. |  |
| 1.13  Unauthorised Access/Information Release | 1. The service provider shall not sponsor any person to visit site   without the authority of the DO or his representative.   1. No individual shall be allowed within the Security Control   Centre or Security Posts without the authorisation of the DO or his representative.   1. No Data, statistics, information or images are to be released   without the authority of the DO or his representative.   1. Visitors to Security Posts / Centre must sign the Visitor Book   acknowledging confidentiality. | The Security Posts and Security Control Centre are restricted areas. Only authorised personnel should be given access. |  |
| 1.14  Service providers Management & Supervision of contract. | 1. A suitably qualified or experienced Contract Manager shall   formally meet with the Designated Officer (DO) monthly.  b. The Contract Manger shall visit site no less than once  every 30 days.  c. Ad hoc visits by service providers’ staff or management,  who do not form part of the work team rota, are not allowed without the prior approval of the DO.  d. The service provider shall appoint a suitably qualified or experienced site-based supervisor, employed separately from a guarding task.  e. Supervisor to be available for weekly scheduled  meeting / briefs with DO, typically 1-hour duration.  f. Contract Manager/Supervisor to provide statistics in line  with the Key Performance Indicators (KPI) and Service Level Agreement (SLA). | These requirements and parameters are measurable within the KPI process. |  |
| **1. Command & Control** | 1. **Requirement** | **Additional Information** | |
| 1.14  Service providers Management & Supervision of contract.  CONTINUED …. | g. Present written report on finds or extraordinary events  within 12-hours to DO.  h. Present KPI statistics weekly to DO.  i. Present SLA statistics monthly to DO.  j. Ensure Assignment Instructions (AI’s) reflect Standard  Operating Procedures (SOPs), are current and meet DO approval.  k. Provision of two authority delivered training or  communications days per calendar year to be made available for site-based staff without loss of service provision |  |  |
|  |
| 1.15  Service provider to supply Staff clothing and Equipment. | 1. Guards and supervisors to be dressed in clean,   presentable uniforms including stout clean footwear.   1. The uniform is to be approved by the DO. 2. Foul weather clothing and appropriate footwear for each   guard and supervisor shall be supplied.   1. High visibility clothing shall be provided for personnel   engaged in access control, security patrols, traffic-control or vehicle search duties.   1. High intensity torches including consumables in sufficient   number to allow the guard to execute their duties at all times.   1. Suitable number of under vehicle search mirrors with   illumination facility including consumables in sufficient numbers to allow the guard to execute their duties at all times.   1. Unofficial Pin badges, tie clips, emblems etc must not be   worn whilst on duty without the approval of the DO.   1. Harness & Fall arresters or any other equipment required   for the safe working at height (Rooftop and Gantry), this equipment must be maintained in accordance with any Health and Safety requirements.   1. Safety helmets, ear defenders, gloves and light eye care   are to be provided for staff involved in escorting contractors. | No unauthorised personal items of clothing or equipment are to be worn or carried whilst on duty.  These requirements and parameters are measurable within the KPI process. |  |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.16  Service provider to align and embrace the MoD Code of Conduct in addition to any internal company Codes of Conduct. | Guards and Supervisors must abide with the basic code of conduct contained within BS 7499 and JSP 440 committing or condoning any one of the following will be regarded as a breach of this code of conduct:  a. Neglecting or, without due cause, failing to carry out promptly and diligently a required task within their job description whilst at work.  b. Failing to comply with the security orders in a way that would potentially lead to a compromise of sensitive information  c. Leaving a place of work during any period of duty without due permission or sufficient cause or failing to work to the agreed shift pattern.  d. Knowingly making or signing any false oral or written statement.  e. Destroying, mutilating, altering or erasing any official document or record.  f. Divulging to any other person who does not need to know, any matter which is protectively marked or is private business of the MoD’s or contractors, past or present.  g. Soliciting or receiving any bribe or other consideration from any person.  h. Failing to account for documents, keys, a pass or passes, money, or property received in connection with their duty and/or the MoD’s business.  i. Being uncivil to persons encountered in the course of their duty or abusing their position of authority in connection with the discharge of the MoD’s business.  j. Acting in a manner reasonably likely to bring discredit upon the MoD, or to fellow employees.  k. Wearing the uniform provided by the Company incorrectly or using MoD equipment without authority.  l. Carrying out or reporting for duty whilst under the influence of alcohol, controlled drugs, or solvents, or consuming any of these whilst on duty. Guards are to advise their supervisor if their performance may be affected by drugs prescribed by a medical practitioner. | Any contravention of the Code is a breach of contract, any member of the service provider’s staff may be refused access to MoD property by the DO.  These requirements and parameters are measurable within the KPI process. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.17  Service provider to align to the MoD Code of Conduct.  CONTINUED…. | m. Failing to report forthwith to the Designated Officer through the Commercial Guarding Management any conviction for a criminal or motoring offence (other than a minor motoring offence, which does not impact on the effective discharge of official duties).  n. Knowingly allow any access to MoD premises by any unauthorised person or persons.  o. Whilst on duty carrying any unauthorised equipment not issued to him/her as part of their duties, (e.g. Multifunction Knife).  p. Failing to report for duty at the correct time and place unless due notice and reasons have been given to their supervisor.  q. Sleeping whilst on duty.  r. Smoking or carrying any smoking materials including matches and cigarette lighters, in any prohibited place where such activities and materials are banned. | Any breach of this Code of Conduct may render the individual to be considered unacceptable for employment on MoD property. In such a case the Contractor will be notified by the DO accordingly and will replace the offending individual forthwith.  These requirements and parameters are measurable within the KPI process. |  |
| 1.18  Service provider to accommodate short notice/short duration requests. | The Designated Officer (following approved protocol) can invoke a Security Enhancement Clause (SEC) requiring additional guards to meet the security requirements of a higher alert state or to cover a specific event  Guards to assist and participate in any training exercises that may be called under the direction of the DO. |  |  |
| 1.19  There may be a requirement to significantly increase guarding numbers, within the contract period, to meet the security requirements of the Pride 2 project. | P2 is a project name for the development and expansion of the RAF Wyton Site. Although no details are confirmed some scenarios and are described in Annex A.  Although it is the Service Provider’s responsibility to estimate the number of guards required to meet the requirement, the standards and tasks detailed within this SOR will be applied to any build within the P2 initiative. | The Authority will ensure early consultation with the Service Provider allowing for a suitable amount of time for planning and recruitment when additional guarding is confirmed. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.20  Service providers to receive briefing from Designated Officer or DO’s representative to cascade to the guard for that day’s duty. | The following list is typical but not exhaustive of the topics to be covered during the brief:  a. Changes to the threat.  b. Alert state.  c. Changes to the normal routine.  d. Planned events.  e. Details of known visitors, special events etc.  f. Any specific areas of responsibility:  g. Passes (personnel/vehicles).  h. Vehicle search.  i. Contractor’s employees/vehicles.  j. Security of building.  k. Communications.  l. Administration.  A Level 5 supervisor grade is to be available no later than 09:30 to receive the brief. This brief can be incorporated within the weekly morning scheduled meeting. | DO or his representative to ad hoc sample staff post briefing, to ensure message has been effectively cascaded and understood. |  |
| 1.21  Service provider to maintain records | These records are typically but not exhaustive:  a. DOB / Incident Book  b. Roster register  c. Key register  d. Passes issued and returned  e. Telephone log  f. Assignment Instructions  g. Staff contact details  h. Security Seal register (Main Register maintained by Security  i. Information Redacted  j. Voice Alarm/ Public Address system announcements  k. Patrol reports  l. Authorised signature list  f. Maintenance reporting Log | DO or his representative to audit no less than once per month, accuracy of records will form part of the KPI.  These records can either be hand-written or entered via a computer and stored electronically. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.22  Guard Force Facilities | The following will be provided by the authority:   1. Heated and well-lit security posts. 2. MoD Telephone. 3. Toilets. 4. Cooking and messing facilities. 5. Site specific Health & Safety training. 6. Washing/Showering facilities 7. Drying Room 8. Furniture including suitable seating 9. Rest/breakout area. | The service provider must ensure their work area is kept clean; this will form part of the KPI.  Guards are expected to have exemplary personal hygiene standards. |  |
| 1.23  Service Providers Responsibilities | The following is the responsibility of the service provider:  a. Cleanliness of the work area.  b. Any transport required.  c. Site specific Health & Safety equipment.  d. To report any damage to equipment, facility or IT to the DO.  e. To strive for zero non-compliance or customer complaints.  To build working relationships with customers:  a. In order to deal with any incidents effectively and tactfully,  using the utmost discretion where required.  b. Complete all tasks as assigned diligently.  c. To liaise with external agencies when requested to do so  by the DO.  d. To assist in the development of Standard Operating  Procedures.  e. Support and adhere to any Security Orders  and Standard Operating Procedures.  f. Training as covered in 1.9. | Forms part of the KPI and contractual agreement for replacement at service providers cost including supplementary cover should it be so required.  Customer relationship forms a measurable within the KPI. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1. Command & Control** | **Requirement** | **Additional Information** | |
| 1.24  Tasking commitment | **Security Control Centre – Pathfinder SAO**   1. Monitor and control CCTV system 2. AACS to be monitored. 3. IDS to be monitored. 4. Key issue and control. 5. Appropriate response to alarms. 6. Incident control and management   **Main Security Post / Secondary Security Post**   1. Baggage scanning/personnel/vehicle searches. 2. Ensure all Protectively Marked Material meets Security   Policy requirements on exit or entry to the facility.   1. Issue temporary personal passes and vehicle permits out   of hours via Visitor Management System (VMS)  **SAO and GAO**   1. Internal & External patrols as defined in Assignment   Instructions | 24-hours / 365 days / year |  |
| **Manning Hours**   1. Main Security Post / Reception excluding Public Holidays. 2. Pass issue to be available Monday to Friday excluding Public Holidays. 3. Escorts to be available Monday to Friday excluding Public Holidays, and to cover ad hoc requests. 4. Secondary Security Post | 24-hours / 365 days / year Information Redacted  Visitors must be attended to in less than 5 minutes  Day shift hours and when required out of normal hours |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.1  Scanning of Mail, Packages. | 1. All mail deliveries are to X-Ray scanned by suitably trained   personnel (1.9) prior to acceptance within the building.   1. Mail suspected of containing prohibited items is to be set   aside in a quarantine area, to be identified by the named recipient. Only the named recipient is authorised the mail, but this is to be witnessed by the X-ray machine operator.   1. Prohibited items are to be removed from the building by   the recipient.   1. In the event of a suspect package being discovered, you   are to invoke the emergency procedure as per the SOP   1. All finds of prohibited items are to be reported to the DO | These requirements and parameters are measurable within the KPI process. |  |
| 2.2  Spot checks of persons entering and leaving. | 1. All visitors and new personnel are to be searched   Information Redacted   1. Carried baggage and items are to be X-Ray scanned for   prohibited items.  c. Guards must be competent in the use of the search equipment and the Search Code of Conduct.  d. Guards are to be confident when conducting random non-contact, visual confirmation searches on persons. For example, asking personnel to empty pockets or bag contents.  e. Guards are to be competent at inspecting documents and notebooks leaving the SAO and be able to recognise protectively marked material and passwords | Searches to be conducted in specially designated areas only.  A Record of Search is to be maintained.  These requirements and parameters are measurable within the KPI process. |  |
| 2.3  Challenging for Prohibited items. | 1. Guards must be proactive in detecting and restricting   prohibited items entering the building.   1. All visitors and contractors are to verbally challenge, in   order to confirm they are not in possession of prohibited items   1. All finds are to be recorded in the Record of Search. | It is important that Visitors and Contractors are made aware of the Prohibited Item List and given an opportunity to check their person, prior to search.  If they identify a prohibited item at this stage, there is no requirement to record as a find. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.4  Media Scanning | 1. All magnetic and optical media is to be virus scanned prior   to entry into the building.   1. All staff will receive appropriate training in the virus   scanning PC by the authority and certified by the DO.   1. Any anomalies or positive results are to be reported to the   DO, ITSO or his representative.   1. Out of hours, the duty investigator is to be called. | These requirements and parameters are measurable within the KPI process. |  |
| 2.5  Mobile Phone/Laptops/Media | 1. Mobile phones are not permitted in the SAO. 2. Laptops are not permitted without the authority of the DO   or ITSO.   1. Guards should have a good understanding of the   Pathfinder Portable Electronic Devices (PED) Policy which controls PEDs in the building.   1. Security Mobile Phones and Mobile Phone Detectors are   accountable items and are to be signed for on issue and on hand over   1. Mobile phone detectors are in use and are to be deployed   under instruction from the DO, this device is to be tested once per day.   1. Laptops leaving the building are only to be released after   appropriate checks of the authorisation documents have been made.   1. Hand carried media is only to be released from the building   after checks of the authorisation documents have been made.   1. All mobiles and laptops must be turned off and stored   outside of the secure area.  i. Personnel, reporting they have inadvertently brought a PED into the secure area, are to be reported to the DO or a member of the Security Section straight away. Out of Hours the Duty Investigator is to be informed. | Training will be provided by the authority.  These requirements and parameters are measurable within the KPI process. |  |
| 2.6  Waste | a. Authorise waste for removal from your area of  responsibility.  b. Shred all paper waste generated within any Security Posts. |  |  |
| c. Destroy by means provided by the authority all classified  waste.  d. Visually confirm recyclable material is free for release. |  |  |
| 2.7  Key issue | 1. Security keys to be controlled, issued and recorded in   accordance with internal processes and JSP440.   1. Key presses/cabinets to be audited at the end of each duty. 2. Any discrepancies must be reported to the DO. 3. Authorised key demanders list to be maintained in date. |  |  |
| 2.8  Guard patrol | 1. Information Redacted 2. Physical patrols of building (internal and external) to be conducted by guards. 3. Security doors to be checked and secured. 4. Security seals to be to doors and equipment when needed 5. Information Redacted 6. Desks are clear of protectively marked material. 7. Security furniture is closed and locked if unattended and the relevant Security Check sheet annotated. 8. Raise report for DO and enter details in the DOB if insecurity is found, removing items for secure storage and leave ‘notice of removal’ slip. 9. Confirm no visitors or un-cleared personnel are present before turning off the visitor warning system. Information Redacted 10. Conduct a full and comprehensive building search when instructed by the DO or in response to Operation Information Redacted or Information Redacted being instigated. 11. Check badges are displayed and in date. 12. Check and observe if un-cleared persons are escorted. 13. Remain vigilant, focused and committed to the prevention and detection of security breaches or weaknesses. | Information Redacted  Information Redacted  These requirements and parameters are measurable within the KPI process. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.9  Visitor Management System (VMS) | * 1. The PC based system VMS will be used to complete the booking in of visitors and contractors into the building at the front and rear entrances.   2. The VMS will be pre-populated by the Vetting office prior to the arrival of any person.   3. Guards are to identify all Visitors and Contractor arriving at Pathfinder by verifying their identity documents and confirming they are expected on the VMS.   4. Once identity is verified the guard is to issue a visitor pass and a lanyard of the appropriate colour dependent on their security clearance level and nationality.   5. If the visitor requires to be escorted, the guard will call the point of contact and invite the visitor to wait to be escorted.   6. Guards to ensure that escort has signed escort orders.   7. At the end of the visit, the guard must retain all passes issued and end the visit on the VMS.   8. All losses of passes or holders must be reported to the Vetting Office for card suspension, with a written report prepared for the DO.   9. Persons who arrive who are not on the VMS are not to be allowed in without authority from the DO or his representative.   10. For VIP visits guards are to produce pre-prepared badges ready for issue without the need for photo capture. VIPs usually escorted by a representative from Command Group who are usually present at the front reception to meet the VIP.   11. Guard supervisor to attend weekly meeting with Visits and Vetting to discuss forthcoming VIP Visits and conferences.   12. Guard supervisor to report any functionality issues with the System and order consumables from supply when required. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.10  Security Seals | a. The service provider is to apply security seals as directed by  the DO or representative. Seal numbers and locations are to be  recorded and the DO is to be informed  b. The service provider shall supply UV fluorescing transparent  self-adhesive seals suitable for electrical outlet screw covers,  also, similar seals suitable for abutting surfaces.  c. The service provider shall also supply a UV light emitting source complete with consumables and maintained in good order. |  |  |
| 2.11  Void Checks | 1. The service provider will inspect and record prior to closure   any voids which have been created by any contractor, these will have been identified in the risk and method statement before work commenced.   1. At cease of the work, guards are to check that the area is   secure and that no signs of tampering are visible outside of the defined are of works as stipulated on the risk & method statement.   1. Guard is to certify that the area has been inspected. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.12  Automated Access Control System (AACS) | * 1. The building has a comprehensive AACS with   approximately Information Redacted   * 1. The AACS also has an electronic muster (automatic   counting out facility) which the service provider will also operate.   * 1. Service provider is to electronically monitor all controlled   entrances and exits for invalid transaction, anti-pass back violations etc.   * 1. Service provider to operate the tiger traps control system.   2. Service provider to ensure correct protocol is observed   prior to opening the ATIC door.   * 1. Service provider to ‘lock down’ in the event of Operation   Information Redacted being invoked at the instruction of the DO.   * 1. Service provider to liaise with Vetting Office and Visits to   ensure road barrier, speed stiles and portals are opened /lifted in a timely and coordinated manner for VIP visits.   * 1. Run end of day visitor reports prior to allowing the red   visitor warning lights to be turned off.   * 1. Prepare passes and lanyards for issue to visitors and   contractors.   * 1. Issue badges to staff who have forgotten them, after   confirming with the Vetting Office staff. | Training to be provided by the authority on systems.  Information Redacted |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.13  Telephone/Intercoms | 1. Service provider will be expected to answer the telephone   within 5 rings and use a scripted announcement.   1. All hoax or suspect calls are to be recorded in the DOB and   reported to the DO or representative.   1. Bomb threats are to be dealt with as per orders and   Assignment Instructions.   1. Emergency calls from internal lifts or refuge areas are to be   dealt with as per authority instructions.   1. Video intercoms and voice only intercoms are used to verify   identity and reason for access,   1. Service provider is the communications conduit between   site and the fire service via the guardroom.   1. A direct line telephone is installed to the guardroom, this   link is to be tested at 23.59-hours each day.   1. Telephones are for official business use only. | Training to be provided by the authority on systems |  |
| 2.14  Two Way Radio | 1. The service provider will only use communication radios   and base station supplied by the authority.   1. Strict radio protocol shall be adhered to at all times, using   approved calls signs and phonetic alphabet in the relaying of information which would otherwise be ambiguous.   1. Radios shall be placed on charge when not in use. 2. Patrolling guards are to carry a radio at all times, but must   not be turned on or used within the building unless in an emergency, this emergency must be logged in the DOB and a written report prepared for the DO.   1. Respond to all emergency calls from other units in range. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.15  Tannoy (Voice Alarm System) | 1. Announcements are only to be made with the authority of   the DO or his representative.   1. Time sensitive announcements must be made with an   accuracy of no less than +/- 1 minute.   1. Only announcements which have been written down to be   read out are to be used.   1. Standard announcements are to be kept updated within the   Security Control Centre.   1. The station Tannoy can be routed throughout the building,   the enabling of this feature is at the discretion of the DO.   1. Announcements are to be kept to an absolute minimum   during conferences or briefings | Training to be provided by the authority on systems |  |
| 2.16  Intruder Detection System | 1. The service provider will monitor all intruder alarm and take   the appropriate action as outlined within Security Orders and SOP should activation occurs including the dispatching of a guard to the area.   1. The system has differing priority signals with differing   physical presence response times:   * Priority 4 - Information Redacted * Priority 3 – Information Redacted * Priority 2 – Information Redacted * Priority 1 – Information Redacted  1. The Intruder Detection System is part of the integrated   Security Management System (SMS), users must log in and be accountable for their actions.   1. The service provider must make staff available for training   to be provided by the authority.   1. All singleton staff must be familiar and competent with this   system.   1. Alarms must be accepted and actioned within Information   Redacted of activation.   1. Information Redacted alarms must be confirmed as being   ‘Set’ before keys are accepted back. | The authority will train and certify staff in the operation of this equipment.  Response times will be tested and form a measurable performance KPI.  Alarm acceptance time will form part of the KPI. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.16  Intruder Detection System  CONTINUED…. | 1. Information Redacted and external plant room doors must   be confirmed as being closed before keys are accepted back.   1. Any ‘Unset’ system must be logged in the DOB and a report   prepared for the DO.   1. Any alarm activations must have a cause attributed prior to   being reset and be fully investigated.   1. Any system faults must be reported immediately. 2. Any faulty circuits can only be omitted after a works request   has been submitted and with the authority of the DO or representative.   1. Cross site systems will also be monitored. 2. External assistance is available via a direct line to the   station guardroom in an emergency.  o. Any work conducted on the system must be logged in the  DOB. | Training to be provided by the authority on systems |  |
| 2.17  CCTV | 1. A sophisticated CCTV system with a combination of   Information Redacted fixed and Information Redacted (PTZ) cameras complete with digital recording is installed.   1. Operators are to be trained in the operation of this system   by the DO.   1. The primary viewing equipment is housed within a bespoke   Security Control Room.   1. Service provider to extract images from the system at the   request of the DO or his representative (either hard copy or optical /magnetic media).   1. Service provider to review recorded images for events when   instructed by the DO or his representative.   1. Service provider is not to let any person have access to any   recorded material without the prior authorisation of the DO or his representative.   1. Service provider shall conduct regular ‘ Information   Redacted as outlined in 2.8 a).   1. Service provider shall confirm the status of all cameras and   functionality at Information Redacted , results to be recorded in the DOB.   1. Any failures shall be reported and entered in the DOB, a   written report to be prepared for the DO.   1. Privacy masking shall be enabled; any inappropriate use of   the CCTV system will not be tolerated.   1. Any work conducted on the system must be logged in the   DOB. | Training to be provided by the authority on systems.  Task reserved for Supervisor.  Inappropriate use of the system will be investigated by the Authority. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.18  Respond to alarms | 1. The service provider is to be first responder to any alarm,   typically, but not exclusive to:   * Disabled toilet alarm * Disabled refuge * Building Management System (BMS) alarms * Intruder Detection System (IDS) * Perimeter Detection System (PIDS) * Access control generated alerts * Personal Attack Button (PAB) Alarm * Fire Alarm * Internal and external Plant alarms * Security Door alarm * Lift Alarms * Plant Alarm   b. Appropriate action as defined within orders and SOPs must be  complied with, any activations and their response are to be recorded in the DOB and a written report prepared for the DO. |  |  |
| 2.19  Escort duties | 1. Cleared guards are to act as escorts when asked to do so by   the DO or his representative.   1. Guards are to escort contractors ensuring that the works   identified in their risk & method statement is conducted as stated.   1. Guard is to remain with the uncleared individuals until escorted   out of the SAO or relieved.   1. Guard is to offer direction, guidance and assistance to queries   asked of him/her. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **2. Internal Tasks** | **Requirement** | **Additional Information** | |
| 2.20  Emergency Procedures | 1. Service provider will be responsible as the Incident   Commander (IC) until relieved by the DO or representative.   1. The IC duties include, but not exclusive to, ensuring that the   IC/Guards:   * + - Call the emergency services     - Generate a muster printout     - Broadcast fire message if required     - Post the guards to point duty guarding exits from the   building   * + - Liaise with Fire Marshalls and coordinate head count in preparation for the arrival of the emergency services (Muster).     - Be a focal point for staff.     - Be the key holder for access to outbuildings.     - Escort emergency services to the alarm point.     - Reset the fire alarm.  1. The Incident Commander is also a focal point within the   Business Continuity Plan (BCP) as the duties are aligned.   1. In the event of Operation Information Redacted being   invoked, all doors are to be closed and secured, access control doors are to be over-ridden and a Broadcast is to be made to all staff to check their area of responsibility, further details will be in orders and Assignment Instructions. | Training to be provided by the authority on this process. |  |
| 2.21  Extraneous Duties | 1. Check exit paperwork for items leaving the building. 2. Conduct byte size checking. 3. Conducting tours of the building. 4. Adjusting the time to maintain accuracy on security equipment i.e. BST/GMT, time to be referenced to station master clock. | Training on changing/adjusting systems time to be given by the authority |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3. External Tasks** | **Requirement** | **Additional Information** | |
| 3.1  Conducting vehicle searches. | 1. The purpose of the vehicle search is to identify:  * The presence of any surveillance equipment. * The presence of items that could be used in the pursuit of crime. * Persons not declared at Main Gate and who do not have passes.  1. All vehicles entering the fenced compound are to be booked   in and the details recorded in the Daily Occurrence Book (DOB).   1. Vehicles entering the ATIC area are to be searched; this will   involve obtaining consent to search, a visual inspection within the cab, engine compartment, boot/rear storage and under body using an appropriate tool or visual observation.   1. Delivery & collection vehicles are to be searched, this will   involve obtaining consent to search, a visual inspection within the cab, boot/rear storage and under body using an appropriate tool.   1. Contractors vehicles are to be searched as d) 2. Disabled vehicles are to be searched as c) when instructed   to do so by the DO.  g. Vehicles with on-board cameras such as dash cams and  reversing cameras must be covered before entry to compound is  allowed. | Failure to obtain vehicle search consent will automatically deny access to the Compound or front of building to that individual and vehicle.  Training will be delivered by the authority in the searching of vehicles and personnel. |  |
| 3.2  Vehicle access control. | 1. Confirm delivery, collection or works has been scheduled by inspecting/cross referencing documentation prior to admittance to the fenced compound. 2. Visually verify/confirm identity by use of video intercom and CCTV. 3. Using Automatic Access Control System (AACS), open gates/barrier. 4. Liaise with Security Control Centre throughout operation. 5. Close gates/barriers as soon as is reasonably practicable 6. Reset security system monitoring gates. 7. Disabled vehicles will be denied access to within 25m of the building if the alert state rises, the DO will confirm. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3. External Tasks** | **Requirement** | **Additional Information** | |
| 3.3  Vehicle egress control. | 1. Carry out tasks as outlined in 3.1 d) excluding under-body. 2. Conduct CCTV sweep of area prior to opening gate/barrier. 3. Using AACS open the gate or barrier. 4. Liaise with Security Control Centre throughout operation. 5. Close gates/barriers as soon as is reasonably practicable.   f. Reset security system monitoring gates.  g. Book the vehicle off site in the DOB. |  |  |
| 3.4  Fence Patrol | 1. Fence to be foot patrolled Information Redacted and   Inspected for signs of damage, tampering, foliage growth, unauthorised signage attached to the security fence, climbing aids in close proximity to the fence etc.   1. Fence to be patrolled at infrequent times during the day and   night in the event that either/or the CCTV and Perimeter Intrusion Detection System (PIDS) fails, Information Redacted 24-hour period is acceptable.   1. Foot patrols without CCTV cover, due to failure inadequate   lighting must be carried out by two persons in Radio contact with the Security Control Centre.   1. Foot patrols shall be conducted by one person under CCTV   surveillance from the Security Control Centre and in Radio communications.   1. Fence to be physically inspected if unexplained PID alarms   are generated and a report generated.   1. Patrol statistics for part of the KPI and must be recorded for   the DO.   1. If the alert state is heightened, the DO will increase the   patrols.   1. Foot patrols can be suspended in the short term with the   agreement of the DO. | These requirements and parameters are measurable within the KPI process. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3. External Tasks** | **Requirement** | **Additional Information** | |
| 3.5  External Escort | 1. Act as escort to un-cleared persons within compound when   requested to do so.   1. Liaise with Security Control Centre to ensure CCTV is   overlooking area where un-cleared person is working.   1. Escort visitors or contractors from the guardroom to site   when requested to do so by the DO or his representative.   1. Act as ‘Banksman’ for reversing vehicles if required. | To ensure no damage is caused to building or plant during vehicle manoeuvres and to assist where necessary. |  |
|  |
| 3.6  Perimeter Patrols | 1. Perimeter within the compound fence line is to be foot   patrolled Information Redacted   1. External doors are to be checked for any insecurity or signs   of surreptitious entry   1. All duct covers are to be checked to ensure tamper evident   seals have not been damaged since the last patrol.   1. All accessible security padlocks are to be checked for   integrity.   1. Confirm external lighting around the building and within the   compound is operating effectively.   1. Visually there are no leaks or hazards that could impinge on   the building functionality,   1. Any issues should be recorded in the DOB, making the DO   aware, if urgent, guard to raise a works request. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **3. External Tasks** | **Requirement** | **Additional Information** | |
| 3.7  Fire Muster/Business Continuity Plan | 1. In the event of an evacuation the muster print-out is to be collected and taken to the muster area. 2. All entrances to the building or are to be point guarded or made secure under the direction of the DO. 3. All gates in the fence line are to be point guarded or made secure under the direction of the DO. 4. Staff are to be familiar with their roles and responsibilities as outlined in orders should the BCP be invoked. 5. Guards are to assist the Fire Service, if safe to do so, under the direction of the DO or IC. |  |  |
| 3.8  Extraneous Duties | 1. Raise & lower flag(s) as and when required. 2. Out of hours, grit path at front and rear entrances to the road   to ensure safe passage to work for staff into the building.   1. Check fire extinguishers. 2. Execute any reasonable request when tasked to do so by   the DO or his representative. |  |  |

Annex A to

Statement of Requirement

Dated 28 Apr 20

**GUARDING CONSIDERATIONS FOR P2**

Information Redacted

Information Redacted

Information Redacted