**Technical Security Contract Specification**

1. General

1.1 This Schedule sets out the Services that will be provided by the Contractor and provides a description of what each Service entails.

1.2 The scope of the Services is to (a) maintain existing and future security equipment at various Bank Premises and (b) supply new security equipment to the Bank as and when required either as upgrades or as new installations.

1. The Services

2.1 The Contractor shall provide sufficient numbers of Staff at all times for the Services, who understand the technical details of the Security Systems, are fully aware of the criticality of the Premises to the nation's infrastructure, who are aware of the sensitivities of the Bank's general working environments and who have the required security clearance (to Government SC standard), skills and training to carry out the Services.

2.2 At all times during core hours the Contractor shall ensure that at least one nominated technician is on site at Head Office and one technician is on site at Debden to respond immediately to reactive maintenance calls and conduct planned maintenance tasks as the reactive workload permits. A dedicated office at Head Office and Debden with computer systems and access to the Bank’s networks will be provided. Response must meet or exceed the KPIs in the Appendix to this Specification. All Staff absenteeism, due to sickness or annual leave of greater than 48 hours must be back filled with a suitable replacement.

2.3. Core site operating hours are between 08:00 to 18:00 for Head Office and Moorgate. For Debden core site operating hours are 07:00 to 17:00. For Leeds core site operating hours are 07:00 to 19:00 from Monday to Friday (inclusive but excluding Bank Holidays), during which times the Contractor will provide the required level of support to ensure Security System failures do not impinge on the Premises' ability to operate efficiently in a secure and safe manner.

The Contractor acknowledges and agrees that it may be required to carry out some routine servicing and reactive fixes in Critical Areas outside of normal working hours.

The Contractor acknowledges and agrees that it will, from time to time, be required to carry out out-of-hours maintenance and testing in order to minimise disruption to the Bank's staff, including.

* The estimated current arrangements for out of hours working is 180 hours per annum.
* where Staff are required to undertake work in areas of high sensitivity;
* to test any areas where disruption would not be accepted during working hours;
* The Contractor acknowledges that the above time periods for out of hours working are indicative only and the Contractor expressly agrees that it is the Contractor's responsibility to establish and determine if these periods are sufficient for the Services required to be performed out of hours. Any changes to the indicative hours above may be proposed by the Contractor for Bank Approval.
* The Contractor shall ensure that maintenance Services do not disrupt and/or adversely affect health and safety within the Premises.
* All out of hours work must be pre-approved by the Bank. The Contractor shall keep track of all out of hours work.

2.4 The Contractor shall ensure that all planned Services comply with the Bank's Security Systems Change Management and Security Systems Patch Policies, as provided to the Contractors by the Contract Owner.

2.5 The Bank may request quotations for new work or amendments to the Security Systems. Within 3 working days of the Contractor receiving such a request from the Bank, it will provide a quotation to the Bank. If a survey is required, the Contractor will have an additional 5 Working Days to conduct it prior to providing the quotation. Once a quotation is approved, the Contractor will send a Risk Assessment Method Statement ("RAMS") within 7 Working Days to the Bank's Contract Owner for Approval prior to any Services commencing on the Premises and these quoted services will form part of the Services and will be subject to the terms of the Agreement.

**Planned Preventative Maintenance ("PPM")**

2.6 The Contractor will provide an auditable record of PPM activities to allow the Bank to measure Key Performance Indicators and ensure service levels are maintained. The minimum Services for Security Systems PPM are as follows:

2.7 The Contractor shall perform the following activities on a daily basis:

* At the start of each day the Contractor's on site engineers must contact all Security Control Rooms to ensure all systems are functioning.
* At the start of each day the Contractor's on site engineers must conduct a review of the Security System server operations and ensure that all internal and external hard drives are functioning.
* At the start of each day the Contractor's on site engineers must review Concept, the Bank's fault reporting system, and respond to any new faults reported out of hours and continue to monitor Concept throughout the day, responding to faults as they arise.
* The Contractor's on site engineers must confirm all servers and workstations are displaying the correct time.

2.8 The Contractor shall perform the following activities on a weekly basis:

* All servers and workstations are connected to the Security Time Server.

2.9 The Contractor shall perform the following activities on a monthly basis:

* Review and update the Spares list.
* Arrange and perform planned preventive maintenance on all Security Systems Equipment and their interfaces for all critical areas:
  + CCTV: cameras should be cleaned, serviced and checked for field of view accuracy
  + Access control: readers should be cleaned, serviced and checked for functionality

Critical areas included, but are not limited to (Critical Areas):

* Perimeter
* Security Control Rooms
* Citadel and Counters
* Parlours
* RNO
* NQR
* RTGS
* Cash Centre
* Data Centres and Comms Rooms

2.10 The Contractor shall perform the following activities regularly at three month intervals:

* Perform general observation patrols of the buildings (general access areas) at Head Office, Moorgate and Debden to identify any health and safety issues and immediate security concerns. Any equipment failures or deficiencies in operation will be recorded in the Bank's fault reporting system, Concept.
* Provide training to control room staff on how to use the security systems.

2.11 The Contractor shall perform the following activities at six monthly intervals:

* Perform planned preventive maintenance on all Security Systems Equipment and their interfaces for all general access areas.
* Arrange and perform planned preventative maintenance on all Security Systems and their interfaces on the Bank's Leeds Cash Centre ("LCC") in accordance, where applicable, with the maintenance guidelines for Head Office and Debden. Estimate for completion 1 day.
* The battery autonomy of all standby power supplies supporting security devices and monitoring systems should be checked on a bi-annual basis to ensure they provide standby power for 100% designated periods. Where dual redundant power supplies are utilised the autonomy must be checked for each individual supply. This does not include the control rooms' main UPS supply which is maintained by the Bank's own engineers
* All access control door break glass aborts should be tested for correct activation and presentation on the monitoring system.
* The Contractor will ensure all Security Systems (Security Applications, Servers, Workstations and Databases) are patched (security and operational) to the latest levels and maintained in accordance with the Bank's IT standards.
* Perform planned preventative maintenance of all intruder detection devices on the Debden fence line.

2.12 The Contractor shall perform the following activities annually:

* All security alarm monitoring devices (active and passive detection devices of any type, including PA buttons) will be tested for activation and presentation on the monitoring system and an auditable record produced for the purposes of KPI measurement. If a device is regularly triggered as part of normal day to day operations there is no need to carry out a separate test so long as the Contractor can produce auditable information.
* Test the access control systems resilience by carrying out a forced failure onto the tertiary server and recovery back onto the primary and secondary servers.
* The Contractor will review the PPM schedule and requirements and notify the Bank of any recommended changes to the programme.
* The Contractor will review and update the Security Systems floor plans and issue an updated version of the system topology.
* The Contractor will review and update door controller and alarm panel firmware.

2.13 The Contractor shall perform the following activities every two years:

* Upgrade the access control system in accordance with the Banks’ requirements, as notified to the Contractor. Labour charges for this task (excluding any hardware or software charges) should be included in this contract.

2.14 The Contractor shall perform the following activities based on a planned schedule:

* Provide engineering resource for monitoring and re-engagement of security equipment during electrical black starts at Head Office (6 Per Annum) and Debden (4 Per Annum).

2.15 All PPM activities will be recorded by the Contractor on the Bank's PPM recording system, Concept situated in the Bank’s Premises. The Contractor will make all auditable reports available to the Bank within 5 Working Days of completion of the works or as requested by the Bank. Any equipment failures or deficiencies in operation will be recorded in the Bank's fault reporting system, Concept.

Within four (4) weeks of the Effective Date, the Contractor will carry out a full audit of the Concept system ensuring all tasks are entered correctly with the agreed level of detail and intervals.

2.16 All Security Systems, should be maintained by the Contractor, at least in accordance with the manufacturer's maintenance guidelines and the Bank's maintenance plan, available on the Bank’s intranet. All such equipment has a manufacturer quoted mean time between failures. The planned maintenance routines shall be carried out by the Contractor more frequently on the components that have been identified as critical to system operation, as per the Critical Areas list, thereby reducing any increased risk of failure. Additionally, as part of the planned maintenance routines the Contractor will also test the integrity of the redundancy built into the Security System.

2.17 All planned maintenance shall, where applicable, be completed by the Contractor to ensure the Bank's security operations are maintained at all times. The areas of operation where this is critical include but are not limited to the following:

* Operation Neutral inspections of Control Room Security System equipment at Head Office, Debden, Moorgate and Leeds; and
* Operation Neutral inspections of Equipment Room rack-mounted Security System equipment at Head Office, Debden, Moorgate and Leeds.

2.18 If any equipment inspection is required which cannot be Operation Neutral in critical areas, the Contractor must agree such inspections with the Bank, at least 48 hours prior to the commencement of the inspection. The Contractor will produce a full method statement outlining the potential or actual operational impact.

Reactive Maintenance

2.19 All failures shall be repaired by the Contractor as indicated in accordance with applicable KPIs dependant on Spares availability and if access to area where the failure has occurred is possible. If access is not possible at the time of the fault being reported, the fault shall be repaired by the Contractor on the next Working Day. If Spares are not available to replace a field device an order for replacement part must be submitted by the Contractor for Approval within 3 Working Days.

2.20 Prior to leaving the Premises after attending a reactive maintenance call out, the Contractor shall conduct a functional test with the relevant Security Control Rooms shift leader(s) to ensure all system functionality has been restored. Fault reports must be provided to the Bank within 48 hours of the fault being reported.

Quality Standards

2.21 Throughout the Term, the Contractor shall hold and maintain all of the following accreditations, and evidence the same to the Bank's satisfaction:

(a) HID Advantage Partner;

(b) Software House C-Cure 9000 Enterprise

(c) Avigilon Platinum or Gold partner;

(d) NSI Gold member;

(e) Pelco Endura Certified Integrator

2.22 The Contractor will provide planned preventative maintenance and reactive maintenance to the electronic Security Systems and field devices in accordance with the security industry standards. The Contractor will manage, oversee and maintain the Bank's Security Systems and will ensure they are kept fully functional and, where appropriate, continually improved throughout the Term.

The below table provides information on the current planned preventative maintenance schedule. This is devised by the Bank and is subject to change.

|  |  |  |
| --- | --- | --- |
| **January** | **February** | **March** |
| HO/MG/DB - Critical areas CCTV & AC | HO /MG/DB - Critical areas CCTV & AC | HO /MG/DB - Critical areas CCTV & AC |
|  | Access Control 12 Monthly | Leeds 6 Monthly |
|  |  | DB Fence line 6 Monthly IDS |
| **April** | **May** | **June** |
| HO /MG/DB - Critical areas CCTV & AC | HO/MG/DB - Critical areas CCTV & AC | HO/MG/DB - Critical areas CCTV & AC |
| HO - 6 Monthly AC - full site | MG - 6 Monthly AC - full site | DB - 6 Monthly AC - full site |
| HO - 6 Monthly CCTV full site | MG - 6 Monthly CCTV full site | DB - 6 Monthly CCTV full site |
| **July** | **August** | **September** |
| HO/MG/DB - Critical areas CCTV & AC | HO/MG/DB - Critical areas CCTV & AC | HO/MG/DB - Critical areas CCTV & AC |
| HO Vault IDS 12 Monthly | DB Vault IDS 12 Monthly | Leeds 6 Monthly |
|  |  | DB Fence line 6 Monthly IDS |
| **October** | **November** | **December** |
| HO/MG/DB - Critical areas CCTV & AC | HO/MG/DB - Critical areas CCTV & AC | HO/MG/DB - Critical areas CCTV & AC |
| HO - 6 Monthly AC - full site | MG - 6 Monthly AC - full site | DB - 6 Monthly AC - full site |
| HO - 6 Monthly CCTV full site | MG - 6 Monthly CCTV full site | DB - 6 Monthly CCTV full site |

2.23 The Contractor will directly provide the following planned maintenance to all equipment which makes up the Security Systems, excluding mains electrical power supplies, environmental controls and network components.

2.24 The power to security supplies, including the main UPS, on the Premises are excluded from the Services. However the Contractor will inform the Bank if system faults and/or failures (including those relating to power supply) are identified and will liaise with Bank staff during rectification by others of faults by other service providers.

2.25 The Services exclude the security network to which the Security Systems are connected. The network includes the Cisco core and edge switches to which the systems are connected as well as network communications link between the four sites. However, it is the Contractor's responsibility to establish that any identified technical problem is network related before it is escalated to the Bank's IT department. The Contractor will work closely with the Bank's IT department to ensure harmonisation of Service provision.

2.26 The Contractor will support the Bank's planned preventative maintenance programmes for IT, power supply and building management services.

2.28 The Contractor will manage all relevant maintenance sub-contractors appointed by the Contractor to provide the Services and shall demonstrate to the Bank that the Bank is receiving best value from each of these sub-contracts.

2.29 Planning and management of PPM visits of sub-contractors to the Premises will also be the responsibility of the Contractor.

2.30 In the event of equipment failure that cannot be rectified by first line response, the Contractor will be responsible for liaising with sub-contractors to ensure that KPIs are met.

2.31 The Security Systems which are the subject of the Services are installed at the Bank's Premises at:

• Bank of England, Head Office, London EC2R 8AH ("Head Office")

• Bank of England, 20 Moorgate, London, EC2R ("Moorgate")

• Bank of England, Printing Works, Langston Road, Loughton, IG10 3NN ("Debden")

• Bank of England, Leeds Cash Centre, King Street, Leeds ("Leeds")

• Bank of England, Sports Centre, Priory Lane, London SW15 5JQ (“Roehampton”)

1. Staff and Resourcing

Core Roles:

1. Contract Manager (Based at Head Office)

2. Senior Engineer (Based at Head Office)

3. Engineer (Based at Head Office)

4. Engineer (Based at Debden)

5. PPM Engineer (Pansite, as PPMs dictate)

* The Contractor shall ensure that there is adequately trained staff on the Contract at all times minimizing key person risk.
* The Contractor shall provide suitably qualified and experienced Staff capable of exercising professional standards of judgment and discretion in relation to maintenance tasks for the Security Systems.
* The Contractor shall provide suitable and sufficient resourcing to facilitate operation of the Security Systems and equipment to effect optimum performance levels of the plant and equipment.
* The Contractor shall provide details of its Key Personnel, together with their CV’s, who shall be responsible for the execution of the contract.
* The Contractor shall provide a statement on his intention to resource fully the efficient operation and maintenance of equipment and plant over the contract period. The Contractor must demonstrate that the resources are sufficient, competent and qualified for this purpose.
* The Contractor is also required to make a statement on their company’s corporate policy towards training personnel for both technical and issues relating to statutory regulations.
* All Staff, prior to carrying out any Services on Bank Premises, will be subject to and have received security vetting clearance.

4. Bank’s Contacts

Accountable Executive: Dominic Whittle

Relationship Manager: David Wetherell

Contract Owner: Zee Anwar

5. Reporting

5.1 Throughout the Term, the Contractor will maintain a record confirming that all Staff have read and are compliant with the Bank's Security Systems Change Management Policy. This record will be reviewed by the Bank annually.

5.2 The Contractor will provide a performance report to the Bank's Contract Owner on a monthly basis. The Contractor shall also provide to the Bank a quarterly report that will include but not be limited to the following information:

• Labour resources

• Health and Safety

• Reactive maintenance

• PPM schedule and progress

• Spares

• Project Works

• KPI measurement (response times, part ordering, reporting and invoicing)

5.3 The Contractor will collate and maintain a Security Systems maintenance programme which will be reviewed monthly with the Bank's Contract Owner every quarter.

5.4 The Contractor shall provide first line support for Security Systems which are managed by external third parties. The Contractor is required to manage these contracts on the Bank’s behalf by carrying out first line diagnostics in the event of a system fault or failure, and if required contacting and working with the responsible third party to resolve the issue. The systems include (but are not limited to):

* The Bank’s Biometric Readers Contract
* The Bank’s Speedgates and Turnstiles Contracts
* The Bank’s Radio System Contract
* The Vehicle Tracking System Contract
* The Vehicle Cash in Transit Radio System Contract
* The Drone Alerting System Contract – (Currently in development)
* The Head Office Yard Door Maintenance Contract
* The Metal Detector Maintenance Contract
* Specialist Entrance Doors Contract
* X-Ray Machines Maintenance Contracts

The Contractor shall provide additional Avigilon Servers at the mark-up agreed at tender stage.

6. Spares

* To minimise down time and inconvenience, the Contractor must hold an appropriate stock of Spares to affect immediate corrective maintenance to essential Services. The Bank's recommended Spares list is set out below.
* The Contractor must advise the Bank of any end of life or obsolete Spares or equipment as part of a regular monthly stock check.
* Within three (3) weeks of the Effective Date, the Contractor will carry out a full audit of current available Spares held in stock at each of the Premises and provide a report detailing any deficiencies in the quantity and type of Spares recommended within relevant Laws.

7. Additional Services

The Bank may require Additional Services relating to the Security Systems. Such Additional Services could include the new UK specification security equipment as installed on site or as required to supply upgrade paths for existing equipment and to be able to supply any new products required by the Bank as and when they enter the market. It may also include enhancements or amendments to the Security Systems from the Contractor.

Such Additional Services may be subject to a further tender process subject to anticipated project cost, in which the Contractor may participate but the Bank does not guarantee that the Contractor will be awarded any further work in respect of Additional Services.

The Bank may submit a request for Additional Services under this Agreement and within five Working Days of receiving the request, the Contractor shall, if necessary, carry out a survey and shall provide a quotation to the Bank within a further three Working Days. Once a quotation is approved by the Bank, the Contractor will send Risk Assessment and Method Statements within ten Working Days to the Bank's Contract Owner for Approval, prior to any Additional Services commencing on site.

Unless otherwise agreed these Additional Services will be deemed Services and be subject to the terms of this agreement upon Bank Approval.

8. Training

The Bank requires the Contractor to keep them informed of new and emerging technology for evaluation to enhance their Security Systems and monitoring and response capability.

At intervals not exceeding four months (the first such four-month interval being the four-month period from the Effective Date), the Contractor shall perform training on operating the Security Systems for Bank appointed Security and Maintenance Staff.

9. Documentation

All documentation relating to the Security Systems from the "as installed" information, asset lists, register of suppliers, systems schematics, configuration information, service & maintenance records and any other relevant documentation in order to develop a comprehensive system asset and connectivity register must be kept updated as part of a formal change management process. This documentation must be updated as part of a change management process and will be officially reviewed by the Bank on a six monthly basis. The Contractor shall ensure that this information is held securely in a locked security cabinet (the standard of which must be agreed with the Bank) located in the Bank's Premises. Documents are held by the Bank and the Contractor jointly for system administration and maintenance purposes. On each anniversary of the Effective Date, the Contractor will generate an index of available documentation that will be updated as system modifications and/or enhancements take place, which will be subject to Audit.

10. Administrative Duties

The Contractor shall perform planning and scheduling of current and future tasks for the Security Systems, including:

* planning and scheduling of current and future tasks, including:
* booking in engineers;
* raising change requests for routine services and reactive fixes in data centres;
* arranging and managing access to restricted areas;
* arranging and managing CEVA and onsite deliveries;
* managing third parties access for service and reactive fixes
* arranging escorts;
* providing quotations;
* running activity reports.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| TYPE | HEAD OFFICE | MOORGATE | DEBDEN | LEEDS | ROEHAMPTON | TOTAL |
| ACCESS CONTROL DOORS | 322 | 121 | 149 | 24 | N/A | 616 |
| ACCESS CONTROL READERS | 376 | 153 | 184 | 34 | N/A | 747 |
| ACCESS CONTROL REPORT SERVER | 1 | N/A | N/A | N/A | N/A | 1 |
| ACCESS CONTROL SERVERS | 2 | N/A | 1 | N/A | N/A | 3 |
| ANALOGUE CCTV CAMERAS | 264 | N/A | 130 | 4 | 2 | 400 |
| BIOMETRIC SERVER | 1 | N/A | N/A | N/A | N/A | 1 |
| BREAKGLASS UNITS (BGU) | 256 | 93 | 73 | 14 | N/A | 436 |
| CCTV SERVERS (EXTERNAL) | 1 | N/A | 1 | N/A | N/A | 2 |
| CCTV SERVERS (INTERNAL) | 16 | N/A | 24 | N/A | N/A | 40 |
| CCTV SERVERS (INTERNAL/EXTERNAL) | N/A | 7 | N/A | 6 | 2 | 15 |
| COLP ALARM RESPONSE WORKSTATION | 1 | N/A | N/A | N/A | N/A | 1 |
| DOMAIN/AD SERVER | 1 | N/A | 1 | N/A | N/A | 2 |
| FENCE LINE DETECTORS | N/A | N/A | 57 | N/A | N/A | 57 |
| INTERCOMS | 42 | 2 | 5 | 45 | N/A | 94 |
| INTRUDER CLIENT WORKSTATION | N/A | N/A | 1 | N/A | N/A | 1 |
| INTRUDER DEVICES | 1277 | N/A | 947 | 361 | N/A | 2585 |
| IP CCTV CAMERAS | 295 | 127 | 495 | 159 | 8 | 1084 |
| LEGACY SECURITY CLIENT WORKSTATIONS | 4 | N/A | 5 | N/A | N/A | 9 |
| LEGACY SECURITY SERVERS | 4 | N/A | 2 | N/A | N/A | 6 |
| REQUEST TO EXIT (RTE) | 224 | 66 | 49 | 8 | N/A | 347 |
| SECURITY CLIENT WORKSTATIONS | 34 | 5 | 23 | 9 | 2 | 73 |
| TURNSTILES/SPEED GATES | 7 | 8 | 18 | N/A | N/A | 33 |
|  |  |  |  |  |  |  |
| \* All figures provided are indicative and may be subject to change. |  |  |  |  |  |  |

**ASSET LIST – TECHNICAL SECURITY- SECURITY SYSTEMS EQUIPMENT**

**SPARES LIST – TECHNICAL SECURITY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **TS/MG** | **DB** | **LCC** |
| Access Reader - HID R40 | 3 | 3 | 2 |
| Access Reader - HID RK40 | 2 | 2 | 1 |
| Access Reader - Morpho Compact | 2 | 0 | 0 |
| Break Glass Units - Green | 5 | 5 | 2 |
| Request For Exit (RTE) - Green Mushroom | 5 | 5 | 2 |
| Lock - EM20 | 2 | 2 | 2 |
| Lock - EM02DS | 2 | 2 | 2 |
| Lock - EM05DS | 2 | 2 | 2 |
| Lock - Abloy Trimec | 2 | 0 | 0 |
| Lock - FF (Glass Door) | 2 | 0 | 0 |
| Lock - EL560 | 1 | 1 | 0 |
| Lock - EL561 | 2 | 2 | 0 |
| Lock - EL402 | 2 | 2 | 0 |
| Door Controller - Edge 4rdr | 4 | 2 | 0 |
| Door Controller - Edge 2rdr | 2 | 2 | 0 |
| Door Controller - Istar Ultra | 1 | 1 | 1 |
| Door Controller Board – Ultra ACM | 2 | 2 | 1 |
| Door Controller Board – Ultra GCM | 2 | 2 | 1 |
| Door Controller Board - RM4 | 4 | 2 | 2 |
| Door Controller Misc - ARM1 | 5 | 5 | 2 |
| Door Controller - I/O Board (1x Input/1x Output) | 2 | 2 | 2 |
| Intruder - PIR Standard | 3 | 3 | 3 |
| Intruder - PIR 360 | 2 | 2 | 0 |
| Intruder - Seismic | 2 | 2 | 2 |
| Intruder - Panic Buttons | 2 | 2 | 1 |
| Intruder Misc - Galaxy Rio Board | 2 | 2 | 2 |
| Intruder Misc - Galaxy Keypad | 1 | 1 | 1 |
| Intruder Misc - 520 Panel | 2 | 2 | 2 |
| Intruder Misc - Ethernet Module | 2 | 2 | 2 |
| Intruder Misc - MOXA | 2 | 2 | 2 |
| CCTV Camera - Avigilon Dome | 2 | 2 | 1 |
| CCTV Camera - Avigilon Bullet | 2 | 2 | 1 |
| CCTV Camera - MultiSensor | 1 | 0 | 0 |
| CCTV Camera - Analogue Boxed | 2 | 2 | 0 |
| CCTV Camera Misc - NVT Balum | 4 | 0 | 0 |
| CCTV Camera Misc - Various Lens | 4 | 4 | 2 |
| CCTV Server Hard Drive - 1TB SAS | 4 | 4 | 2 |
| CCTV Server Hard Drive - 2TB SAS | 4 | 4 | 2 |
| CCTV Server Hard Drive - 3TB SAS | 4 | 4 | 2 |
| CCTV Server Hard Drive - 6TB SAS | 4 | 4 | 2 |
| CCTV Server Hard Drive - 10TB SAS | 2 | 2 | 2 |
| CCTV Server Hard Drive - 1TB SATA | 1 | 2 | 0 |
| CCTV Server Hard Drive - 2TB SATA | 2 | 2 | 2 |
| Intercom - Stentofon Phone | 1 | 0 | 1 |
| Intercom - Stentofon IP-Video Intercom | 2 | 0 | 1 |
| Intercom - Commend Unit | 0 | 2 | 0 |
| Intercom - Commend WS Phone | 0 | 1 | 0 |

\* All figures provided are indicative and may be subject to change.