Britam

With you every step of the way

REQUEST FOR PROPOSAL

REQUEST FOR PROPOSAL FOR SUPPLY, INSTALLATION, TESTING, COMMISSIONING AND MAINTENANCE OF SECURITY EQUIPMENT AT BRITAM CENTRE

RFP-2024-001/0005

RELEASE DATE: 15th January 2024

CLOSING DATE: 02nd February 2024 5.00 PM EAT

Table of Contents

EXPRESSSION OF INTENT TO PARTICIPATE IN TENDER 4

1 INTRODUCTION 6

1.0 Purpose of the Tender 6
1.1 Acknowledgement of Bidding Documents 6
1.2 Point of Contact 7

2 ABOUT BRITAM HOLDINGS PLC.. 7

2.0 Organization Profile.. 7
2.1 Britam Vision.. 8
2.2 Britam Mission 8

3 OVERVIEW OF THE PROPOSAL 9

3.0 Overview ....Error! Bookmark not defined.
3.1 Objective of the RFP 9
3.2 Scope of Work 9
3.3 Qualifications ....Error! Bookmark not defined.

4 FORMAT OF RESPONSE TO TENDER.. 34

4.0 Information to be provided by bidders. 34
4.1 General Information about the firm 34
4.2 Bid Preparation and Submission...35

5 GENERAL CONDITIONS OF CONTRACT 35

5.1. INTRODUCTION 35

5.2. AWARD OF CONTRACT 36

5.3. APPLICATION OF GENERAL CONDITIONS OF CONTRACT....................... 36

5.4. BID VALIDITY PERIOD 36

5.5. NON-VARIATION OF COSTS.. 36

5.6. DELAYS IN THE BIDDER'S PERFORMANCE.. 36

5.7. LIQUIDATED DAMAGES FOR DELAY 37

5.8. GOVERNING LANGUAGE 37

5.9. APPLICABLE LAW 37

5.10. SUCCESSFUL BIDDER'S OBLIGATIONS 37

6 EVALUATION PROCESS AND CONSIDERATION .... ERROR! BOOKMARK NOT DEFINED.

7 BRITAM SUPPLIER CODE OF CONDUCT.. 38

7.1 GENERAL 38
7.2 PROVISIONS 38
7.2.1 Relations with competitors..*38*
7.2.2 Bribes, Conflicts of Interest, Gifts and other Courtesies *38*
7.2.2.1 Bribes...38

7.2.2.2 Gifts and other business courtesies...39
7.2.2.3 Conflicts of Interest...39
7.2.3 Compliance and implementation 40
7.2.3.1 Licenses and Returns...40
7.2.3.2 Taxation, Financial Integrity, and Retention of Records 40
7.2.4 Violations..40
7.2.5 Variations 41

EXPRESSSION OF INTENT TO PARTICIPATE IN TENDER

This form is to be completed on receipt of the tender document from Britam Holdings Plc.

This page is to be completed immediately and scan copy in PDF format e-mailed to Procurement tenders@britam.com. The data contained in this form will be used to send out any addenda that may arise. Firms that do not register their interest by completing this form may not be sent addenda that may arise.

Name of the firm's representative completing this form:

____

____

Firm's Name:

____

Address:

____

Tel No:

____

Email Address:

____

Signature: ___________________________________Date:

____

Signed by (Name):

____

Position in Firm:

____

1 INTRODUCTION

1.0 Purpose of the Tender

The Britam Holdings Plc ("Britam") invites qualified firms to submit their proposals for Supply, Installation, Testing, Commissioning and Maintenance Of Security Equipment At Britam Centre.

This Request for Proposal (RFP) is being made available to interested service providers on an open tender basis. This document is intended to provide vendors with sufficient understanding of the Britam's requirements to enable them to respond.

For the purposes of the RFP, it is necessary to disclose information in this document, and its schedules, which is considered confidential and should therefore not be used (otherwise other than in furtherance of this tender) or disclosed to any third party without explicit prior written consent of Britam.

Britam on its part also acknowledges that it is requesting through this RFP for information that is confidential and therefore commits in equal terms to reciprocal confidentiality.

1.1 Acknowledgement of Bidding Documents

Britam invites proposals for **Supply, Installation, Testing, Commissioning and Maintenance of Security Equipment at Britam Centre** in accordance with the requirements set out in this document. Within **three (3) working days** of receipt of the RFP, the Bidder is required to acknowledge receipt of the RFP and notify his intention to submit a bid by email to Britam at tenders@britam.com. The mail will include the signed registration template on Page 4 of this document.

Working days are defined as being any day of the week between Monday and Friday (0800 – 1700 Hrs) excluding weekends and gazetted public holidays in the Republic of Kenya).

Failure to do so shall be perceived as an intention not to submit a bid and the Bidder will be eliminated from the bid process and required to destroy the RFP document in keeping with confidentiality requirements.

1.2 Point of Contact

All enquiries or correspondence concerning the details of this tender should be addressed, in the first instance by e-mail to: tenders@britam.com . The subject on the email should be **"CLARIFICATION ON THE RFP FOR SUPPLY, INSTALLATION, TESTING, COMMISSIONING AND MAINTENANCE OF SECURITY EQUIPMENT AT BRITAM CENTRE".**

- All responses from Britam to the Bidder shall be channelled through the Procurement Officer.
- It is the responsibility of the Bidder to obtain any further information required to complete this RFP.
- Any clarification request and their associated response will be circulated to all Bidders.
- All clarifications must be sought at the latest 5 days prior to the close of the RFP.

2 ABOUT BRITAM HOLDINGS PLC

2.0 Organization Profile

Britam Holdings PLC ("Britam") is a leading diversified financial services group, listed on the Nairobi Securities Exchange. The group has interests across the Eastern and Southern Africa region, with operations in Kenya, Uganda, Tanzania, Rwanda, South Sudan, Mozambique, and Malawi. The group offers a wide range of financial products and services in Insurance, Asset management, Banking and Property. For more information, please visit http://www.britam.com.

The Group offers a wide range of products and services to individuals, small businesses, corporations, and government entities. The range of products includes life insurance, pensions, health insurance, and general insurance through its insurance businesses in the region. The financial solutions which include, unit trusts, investment planning, wealth management, offshore investments, retirement planning and discretionary portfolio management which are offered through its asset management business. In addition, the company carries out property development, and has substantial investments in the banking sector. For More information, please visit http://www.britam.com

2.1 Britam Vision

To be the LEADING diversified financial services company in our chosen markets across Africa.

2.2 Britam Mission

Providing you with financial security EVERY STEP OF THE WAY.

3 OVERVIEW OF THE PROPOSAL

3.0 Objective of the RFP

The selected vendor will be required to.

- Supply, Install, Test, Commission and Maintain the Security Equipment at Britam Tower

3.1 Scope of Work

Scope of work under this section covers:

i. The provision of labor, tools, material, and performance of work necessary for the design, manufacture, quality assurance, quality control, assembly, testing, delivery at site, site storage and preservation.

ii. Installation & commissioning.

iii. Performance & acceptance testing both at the Factory/dealership and at site.

iv. Training of Employer's security personnel.

v. Handing over to Employer and guarantee of the complete system, as per specification hereunder, each complete with all accessories.

vi. Supply of spare parts and warranting trouble free safe operation of the installations.

vii. Providing maintenance support (Including supply/replacement of spares) during the warranty period and, if desired by the Employer also during post warranty period.

viii. Installation and commissioning of the local area network (Hardware, software, and cabling) on which the system will run.

ix. The contractor shall provide all the required equipment and services, whether explicitly mentioned in these specifications or not to fulfill the intent of the specification and to ensure the completeness, operation and maintainability of the system at no extra cost to the Employer.

x. The Tenderer is required to submit with their offer the detailed specifications, drawings, catalogues, brochures etc. for the equipment they intend to supply.

xi. It shall be in the scope of the tenderer to acquire any requisite authorizations or licensing from local authorities where applicable, that may be required in the course of the project.

xii. The Tenderer shall be required to present information along with their offers as follows:

- Shortest possible delivery period of the product.
- Information on proper representative and/or equipped local workshop for back-up service/repair and certified personnel including their names and addresses.

xiii. Installation of the Server Workstations inclusive of the attendant operating software, management software and necessary peripherals such as the mouse, keyboard and connection to a power socket outlet.

xiv. Installation of Client Workstations inclusive of the attendant operating software, client management software and necessary peripherals such as the mouse, keyboard and connection to a power socket outlet.

xv. Installation and termination of PoE switches inclusive of all attendant Category 6a Ethernet cables, all required media converters and ftp cables.

xvi. Conduct FATs at manufacturers/appointed distributor premises witnessed by BRITAM Consultants.

xvii. Conduct Site Acceptance Tests as witnessed by BRITAM Consultants.

xviii. Conduct comprehensive training of BRITAM Engineers and Staff.

xix. Providing maintenance spares.

xx. Providing maintenance tools.

xxi. Providing at least 2-year warranty on all equipment.

xxii. The contractor shall ensure that before the completion of the project, at least four copies of the relevant manuals and documentation, including as built drawings are availed to BRITAM in hard copy and soft copy forms.

EQUIPMENT SPECIFICATIONS

1. Workstation:

- Tower PC.
- Processor: Intel Core i7, 3.40GHz Quad Core.

- Ram: 8GB DDR3/4.
- Storage: 1TB HDD/SSD.
- DVD-ROM Optical Drive.
- NVidia K620 (to Include DP to DVI-D SL and DVI to VGA Adaptors) x1
- Keyboard x1.
- Mouse x1.
- 22" Monitor x1.

2. **Server:**
   Technical Specifications:
   - Processor type/Name: Intel.
   - Processor family: Intel® Xeon® Scalable 8100/8200 series - Intel® Xeon® Scalable 3100/3200 series.
   - Processor core: 7 to 24 cores.
   - Processor cache: 8.25 - 38.50 MB L3.
   - Number of processors: 2.
   - Processor speed: 3.9 GHz, minimum.
   - Maximum memory: 3.0 TB with 128 GB DDR4.
   - Memory slots: 24 DIMM slots.
   - Memory type: DDR4 Smart Memory and Intel® Optane™ persistent memory.
   - Memory, standard: 3.0TB (24 X 128 GB) LRDIMM.
   - Drive Supported: 4 LFF SAS/SATA, 8 SFF SAS/SATA + 2 NVMe, 10 SFF SAS/SATA, 10 SFF NVMe, 1 SFF or 1 Dual UFF rear drive optional.
   - NVDIMM rank: Single rank.
   - NVDIMM capacity: 16 GB.
   - Security: Optional locking Bezel Kit, Intrusion Detection Kit.
   - Infrastructure management: iLO Standard with Intelligent Provisioning (embedded), OneView Standard.
   - Expansion slots: 3.
   - Network controller: Embedded 4 X 1GbE Ethernet Adapter or Flexible LOM and optional PCIe stand-up cards, depending on model.
   - Storage controller: Smart Array S100i and/or HPE Essential or Performance RAID controllers, depending on model.
   - System fan features: Hot-plug redundant standard.
   - Form factor: 1U

3. **Network Switch (Managed):**
   Switches Feature:
   - 8 Gigabit Ethernet Full PoE+ ports with line-rate forwarding.
   - 2 fixed 1 Gigabit Ethernet Small Form-Factor Pluggable (SFP)/ RJ 45 Combo uplinks.
   - Perpetual PoE+ support with a power budget of up to 740W.
   - CLI and/or intuitive web UI manageability options.
   - Network monitoring through sampled flow (sFlow).

- Security with 802.1X support for connected devices, Switched Port Analyzer (SPAN), and Bridge.
- Protocol Data Unit (BPDU) Guard.
- Device management support with over-the-air access via Bluetooth, Simple Network Management.
- Protocol (SNMP), RJ-45 console access.
- Reliability with a higher Mean Time Between Failures (MTBF) and an enhanced limited lifetime warranty.
- support (E-LLW).

4. Data Cabinet:

- 42U (600 x 1000mm) Mesh Door Server Rack cabinet.
- Mounting profile's position/s: front & rear
- Construction: bolted
- Front door: mesh
- Side panels: lockable/removable, solid with vents
- Cable entry: top, bottom
- Ventilation: top, small vents to side panels
- Lock positions: front door, rear door, side panels.

5. LPR System:

a) Camera:

- Image sensor: 1/2.8" progressive scan RGB CMOS
- Lens: 18–137 mm, F2.9–4.0 Horizontal field of view: 16°–2.3° Vertical field of view: 9.6°–1.3° Installation focus, auto-iris, automatic day/night Thread for 62 mm filters, max filter thickness: 5 mm.
- Day and night: Automatically removable infrared-cut filter in day mode and infrared-pass filter 720 nm in night mode.
- Minimum illumination Color: 0.16 lux at 50 IRE F1.4 B/W: 0.03 lux at 50 IRE F1.4, 0 lux with IR illumination on
- Shutter speed: 1/66500 s to 1 s

b) License Plate Capture:

- Detection range: Day: 20–100 m (66–328 ft) Night: 20–50 m (66–164 ft) Night detection range up to 100 m (328 ft) with optional accessory AXIS T90D20 IR-LED Illuminator.
- IR illumination: OptimizedIR with power-efficient, long-life 850 nm IR LEDs with adjustable angle of illumination and intensity. Range of reach 40 m (131 ft) in wide field of view and 50 m (164 ft) in full tele view, or more depending on the scene
- Vehicle speed: Up to 130 km/h (81 mph) with optional edge analytics Up to 250 km/h (155 mph) with server-based analytics Coverage Single Lane with optional edge analytics Two lanes with server-based analytics.

- Installation: Mounting height Up to 10 m (33 ft) Distance from road: Up to 10 m (33 ft) Camera detects tilt and roll angle automatically Built-in licence plate capture assistant optimizes video settings based on mounting height, distance to vehicle, and expected vehicle speed

c) System on chip (SoC)

i) Memory - 1024 MB RAM, 512 MB Flash.

ii) Video

- Video compression: H.264 (MPEG-4 Part 10/AVC) Baseline, Main and High Profiles Motion JPEG.
- Resolution: 1920x1080 HDTV 1080p to 160x120 Maximum pixel density with 8x optical zoom: 25 m (82 ft): 1912 px/m 50 m (164 ft): 956 px/m 250 m (820 ft): 191 px/m
- Frame rate: With WDR: Up to 25/30 fps (50/60 Hz) in all resolutions Without WDR: Up to 50/60 fps (50/60 Hz) in all resolutions
- Video streaming: Multiple, individually configurable streams in H.264 and Motion JPEG Axis Zipstream technology in H.264 Controllable frame rate and bandwidth VBR/ABR/MBR H.264
- Image settings: Saturation, contrast, brightness, sharpness, Forensic WDR: Up to 120 dB depending on scene, defogging, white balance, day/night threshold, exposure mode, exposure zones, compression, mirroring of images, electronic image stabilization, barrel distortion correction, text and image overlay, dynamic text and image overlay, privacy masks Rotation: auto, 0°, 180° Scene profiles: license plate, forensic, vivid, traffic overview.
- Pan/Tilt/Zoom: 8x optical zoom, preset positions.

iii) Network

Network protocols:

- IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTP/2, HTTPS, TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP® , SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, NTS, RTSP, RTP, SRTP/RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, ICMP, DHCPv4/v6, ARP, SSH, LLDP, CDP, MQTT v3.1.1, Secure syslog (RFC 3164/5424, UDP/TCP/TLS), Link-Local address (ZeroConf)

System integration Application Programming Interface:

- Open API for software integration, including VAPIX® and One-click cloud connection ONVIF® Profile G, ONVIF® Profile M, ONVIF® Profile S, and ONVIF® Profile T,

Event conditions:

- Analytics, edge storage events MQTT subscribe Supervised external input, virtual inputs through API, shock detection, video motion detection, audio detection, active tampering.

Event actions:

- Pre- and post-alarm video buffering File upload: FTP, SFTP, HTTP, HTTPS, network share and email MQTT publish Notification: email, HTTP, HTTPS, TCP, and SNMP trap.
- Data streaming: Event data
- Built-in installation aids: License plate capture assistant, remote zoom, pixel counter, leveling assistant, autorotation

Casing:

- IP66- and NEMA 4X-rated, IK10 impact-resistant aluminum enclosure with integrated dehumidifying membrane, IK08 impact-resistant glass front window, weathershield with black anti-glare coating Wind survivability 60 m/s (134 mph) Color: Dark Gray NCS S 5502-B (Weathershield: Black).
- Sustainability: PVC free, 5% recycled plastic.

Power:

- Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3 Typical 7.7 W, max 12.95 W 20–28 V DC, typical 7.8 W, max 13.5 W 20–24 V AC, typical 12.4 V A, max 20 V A.

Connectors:

- Shielded RJ45 10BASE-T/100BASE-TX PoE IDC punchdown connector DC Power connector Terminal block for two configurable supervised inputs / digital outputs (12 V DC output, max. load 50 mA) 3.5 mm mic/line in.

IR illumination:

- OptimizedIR with power-efficient, long-life 850 nm IR LED’s with adjustable angle of illumination and intensity. Range of reach 40 m (131 ft) in wide field of view and 50 m (164 ft) in full tele view, or more depending on the scene.

Storage:

- Support for microSD/microSDHC/microSDXC card Support for SD card encryption (AES-XTS-Plain64 256bit) Recording to network-attached storage (NAS).

Operating conditions:

- -40 °C to 60 °C (-40 °F to 140 °F) Maximum temperature according to NEMA TS 2 (2.2.7): 74 °C (165 °F) Humidity 10-100% RH (condensing).

Approvals:

EMC:

- EN 55032 Class A, EN 50121-4, IEC 62236-4, EN 55024, EN 61000-6-1, EN 61000-6-2, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, RCM AS/NZS CISPR 32 Class A, KCC KN32 Class A, KN35, EAC.
- Safety:
- IEC/EN/UL 62368-1, IEC/EN/UL 60950-22, EN/IEC 62471, IS 13252
- Environment:
- EN 50581, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78, IEC/EN 60529 IP66, IEC/EN 62262 IK10

body, IK08 glass, NEMA 250 Type 4X, NEMA TS 2 (2.2.7-2.2.9) Network NIST SP500–267.

6. Monitors:

a) Display

- Panel Technology: VA with Direct LED backlights.
- Active Screen Area (W x H): 1,428.5 x 803.5 [mm].
- Screen Size [inch/cm]: 65 / 164.
- Brightness [cd/m²]: 350, 280 (shipment setting).
- Contrast Ratio (typ.): 4000:1.
- Viewing Angle [°]: 178 / 178 (at contrast ratio > 10:1).
- Colour Depth [bn]: 1.073 (10bit).
- Response Time (typ.) [ms]: 8 (grey-to-grey).
- Haze Level [%]: Pro (44).
- Supported Orientation: Landscape.

b) **Resolution**

- Native Resolution: 3840 x 2160
- Supported Resolutions: 4096 x 2160; 3840 x 2160; 1920 x 2160; 1920 x 1200; 1920 x 1080; 1680 x 1050;1600 x 1200; 1440 x 900; 1400 x 1050; 1280 x 1024; 1280 x 800; 1280 x 720; 1024 x 768; 800 x 600

c) **Connectivity**

- Input Video Digital: 2 x DisplayPort (with HDCP); 3 x HDMI (with HDCP).
- Input Audio Analogue: 1 x 3,5 mm jack.
- Input Audio Digital: 2 x DisplayPort; 3 x HDMI.
- Input Control: 1 x LAN 100Mbit; 1 x Remote Control (3.5 mm jack); 1 x RS232.
- Input Data: 1 x microSD (Value); 1 x USB 2.0 (Downstream); 1 x USB 2.0 (MediaPlayer); 1 x USB Type-B (Upstream); 2 x USB 2.0 (Compute Module, 1 x 5V/2A powered).
- Output Video Digital: 1 x DisplayPort (loop through: DisplayPort, OPS slot-in PC).
- Output Audio Analogue :1 x 3,5 mm jack.
- Output Control: 1 x LAN 100Mbit.

d) **Sensors**

- Ambient Light Sensor: Integrated, triggered actions programmable
- Human Sensor: Optional, external, 4-5m range, triggered actions programmable.
- Temperature Sensor: Integrated, 3 sensors, triggered actions programmable.

- NFC Sensor: Integrated, 2cm range, free NEC Android App required.

e) Electrical

- Power Consumption [W]: 200 Eco, 255
- Power Savings Mode [W]: < 0.5; < 2 (Networked Standby)
- Power Management: VESA DPMS

f) Environmental Conditions

- Operating Temperature [°C]: +0 to +40
- Operating Humidity [%]: 20 to 80

g) Mechanical

- Ingress Protection IP5x (front); IP2x (back)

h) Media Player

- Supported Image Formats: JPG (baseline, progressive, RGB, CMYK); max. resolution 5000 x 5000; PNG (interlace, alpha channel); max. resolution 4000 x 4000.
- Supported Video Formats: MP4 / MOV / FLV (video H.264, audio MP3, AAC); max. resolution 1080p at 30 Hz, 1080i at 60 Hz; MPG (video mpeg1/2, audio mpeg audio layer2/3, AAC-LC); MP @ ML, MP @ HL; WMV (video H.264, wmv advanced L3, wmv simple / main, audio mp3 wmv std); max. resolution1080p at 30 Hz, 1080i at 60 Hz.
- Supported Audio Formats: MP3 (MP3); max. bitrate 320 kBit/s; WAV (LPCM); max. 48 kHz sampling.
- Supported File Storage / File System: MicroSDHC / FAT16, FAT32; USB 2.0 / FAT16, FAT32

i) Additional Features

- Safety and Ergonomics: CE; EAC; EMC Class B; FCC; SASO; TÜV GS; UL/C-UL or CSA; VCCI.
- Audio: Integrated Speakers (10 W + 10 W); Optional Speakers (15 W + 15 W).
- Operating Hours: 24/7

7. Key Management System:

a) General

- Keys readily available 24/7 or as per curfew.
- Access by Authorized users only.
- 7" touch screen.

- Full audit trail of all users and key transactions.
- Secure storage and management for 180 keys.
- Access via PIN code, card reader and biometric reader.
- Battery backup.
- Soft close-down with no data loss in the event of long-term power failure.

b) Standalone

- Operate entirely independent of other IT systems.
- Standalone 'plug and play' system.
- No network, PC or external connection required.
- USB port for import/ export of reports via memory stick.
- Automatic data back up to removable SD card.

c) Networked

- Full network capability and web management.
- Centralized administration and reporting.
- Web based for remote administration.

d) Other Features

- Reason/Fault logging and Access Schedules.

8. Radio Communication:
Digital Mobile Radio (DMR) Portable:

a) Connection:

- VHF Band, 5 W.
- UHF Band, 4 W
- Colour screen.
- Full keypad.
- 1000 channels.
- Voice and Data Integrated Wi-Fi.
- Canned Text Messaging.
- Freeform Text Messaging.
- Work Order Ticketing.
- Multi-constellation GNSS.
- High Efficiency GNSS.
- Event-Driven Location Update.
- Bluetooth Audio.
- Bluetooth Data.
- Bluetooth Permanent Discovery Mode.
- Bluetooth Indoor Location Tracking.
- Voice Announcement.
- Text to Speech.
- Home Channel Reminder.

b) AUDIO

- Intelligent Audio.
- IMPRES Audio.
- SINC+ Noise Cancellation.
- Acoustic Feedback Suppressor.
- Microphone Distortion Control.
- User-Selectable Audio Profiles.
- Switch Speaker.
- Trill Enhancement.

c) CUSTOMISATION

- Multi-Button PTT.
- Programmable Buttons.
- Emergency Button

d) MANAGEMENT

- Radio Management.
- Over-the-Air Programming.
- Over-the-Air Software Update.
- Battery Management.
- Over-the-Air Battery Management.

e) SAFETY

- Integrated Accelerometer - Man Down
- Lone Worker
- Basic Privacy
- Enhanced Privacy.
- AES Encryption
- Transmit Interrupt
- Emergency
- Emergency Search Tone
- Remote Monitor
- Radio Disable / Enable.
- Waterproof to IP68.
- Rugged to MIL-STD 810

f) SYSTEMS

- Dual Capacity Direct Mode.
- Conventional.
- IP Site Connect.
- Capacity Plus.
- Capacity Max.
- Connect Plus.

g) BLUETOOTH SPECIFICATIONS

Version: 4.0
Range: Class 2, 10 m
Supported Profiles: Bluetooth Headset Profile (HSP), Serial Port Profile (SPP), fast push-to-talk.
Simultaneous Connections: 1 x audio accessory and 1 x data device
Permanent Discoverable Mode.

h) Wi-Fi SPECIFICATIONS

Standards Supported: IEEE 802.11b, 802.11g, 802.11n.
Security Protocol Supported: WPA, WPA-2, WEP.
Maximum Number of SSIDs: 128 (64 for LKP and NKP models).

i) ENVIRONMENTAL SPECIFICATIONS

Operating Temperature: 2 -30 °C to +60 °C
Storage Temperature: -40 °C to +85 °C
Electrostatic Discharge: IEC 61000-4-2 Level 4
Dust and Water Intrusion: IEC 60529 - IP68

9. Security Door (Single Leaf):

a) General Description

- The door leaf to be of two 1.25 mm thick galvanized steel sheets with vertical and horizontal steel reinforcements for optimal security structure.
- The door leaf to be filled with Rockwool or honeycomb for thermal and acoustic insulation.
- The door leaf to be of 50 mm minimum thickness.
- The door shall have a telescopic bottom insert to enable easy adjustment during installation.

b) Locking System

- A -4way door lock system, with four 10 mm diameter front bolts and spring-loaded latch.
- One bottom hook reinforcement mechanism.
- Upper and rear 13 mm bolts operated by the lock, rear hook fixed bolt.
- Cylinder protector to prevent picking and drilling as well as forcing of the lock cylinder.

c) Vertical Stiffeners

- 1.25mm galvanized steel stiffeners to give a stronger shape.

d) Insulation

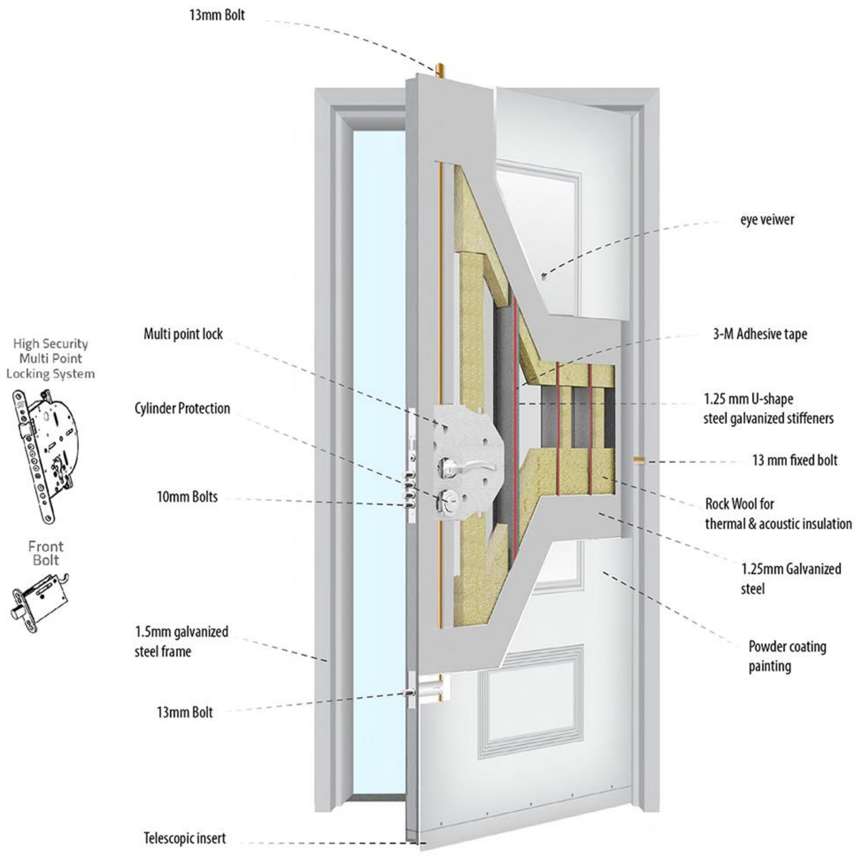
- Rock wool to give high thermal and acoustic insulation.

e) Frame

- Construction frame to be of 1.5 mm thick galvanized steel.
- The frame is mounted directly on the wall with anchors and cemented to the building structure.

f) Door Finishes

- Powder coating *(Color to be advised).*



10. AIR CONDITIONING:

SPLIT SYSTEM

Supply and install a split air-conditioning unit **inverter type** complete as described below.

The outdoor unit shall be mounted on the wall and be provided with purpose-made aluminum painted steel angle iron frame cage complete with anti-vibration rubber mountings. The outdoor unit to match the cooling coil unit.

The indoor unit shall be wall mounted type using bolts, nuts, spring washer and plate washer on the position shown on the approved working drawings. The indoor unit shall be capable of removing microscopic contaminants and dust using reusable filter.

The system to be supplied complete with the following:

- Fully charged with R410A gas.
- A wireless remote control.
- Ground mounting kit.
- Interconnecting piping with flared connections.
- Wired controls.
- Low temperature kit.
- Auto Restart.
- Time delay safety function.
- Service valves.
- 3-step fan speed.

11.2 kW high wall mounted Inverter type split unit complete with its outdoor, the units (Duty & standby).

1 Phase Power protection unit as Sollatek or its equivalent.

1 Phase power isolators as Clipsal/Katko or equal and approved.

11. TRAFFIC ARM BARRIER (6 Meters):

The Barrier shall have an aesthetic appearance, a weather-proof outdoor cabin, a powerful engine, and produced to international quality standards.

Shall have photocells on the barrier detect vehicles passing through, preventing the barrier lever from closing and any possible accidents that might arise.

Shall be controlled with remote controls, manual buttons, card readers and license plate recognition.

Shall be integrated to the Security Management System.

Specifications:

Opening time: 5.5 seconds
Operating Voltage: 220 V (±) (AC) 50/60 Hz.
Max. Arm Length: 6 Meters
Minimum Motor Power: 150 Watt
Daily Operation Cycles Min.: 1545 Cycle
Noise Level: ≤62 dB
Accessories: Traffic Light, Programmable Logic Controller, Photocells.
Operating Temperature: -20 °C / +50 °C
Safety Class: IP55

12. SECURITY MANAGEMENT SYSTEM SOFTWARE:

Integrated Security Management Software.

The purpose of Integrated Security and Decision Management Software (ISMS) is to centralize security operations in a single interface (integrating all the security and safety equipment) and to reduce operational costs and operator response times by having the operators following alarm & event management workflows based on standard procedures.

Minimum Requirement
The ISMS shall be the "Common Operational Picture" (COP), i.e., the single software interface that allows command and control of all security & safety systems, by integrating:
Alarms:
▪ Reception & Multi-User Queuing ▪ Prioritization ▪ Clustering (by site)
Video: "live", "pre-alarm" and "post-alarm" video, video-wall content management;
Maps:
▪ Integration with an external GIS[1] platform, like Google Maps or other; ▪ Importing and configuration of site floor plans or sector plans;
Process Guidance Workflow: The ISMS shall incorporate the step-by-step instructions that shall guide the ISMS operators in handling an alarm or event, shall be fully customizable according with the standard operating procedures (SOPs) of the organization.
The ISMS **Process Guidance Workflow** shall allow for:
▪ **Active content**: it shall be possible to add active content to the workflow instructions or steps in the form of images (photos), video and audio, device status (alarm panel and/or I/O status, for example), record data retrieved from an Access Control System database, etc.;
▪ **Device interaction**: it shall be possible to interact, within the workflow, with security, safety, building management and VoIP devices: activating or deactivating an intrusion zone; arming or disarming an alarm panel, requesting "live" or "pre-alarm" video from a CCTV camera; switching on/off building illumination; requesting the Access Control System for the opening of a door or turnstyle; answering a call from, or calling, an internal or external VoIP extension or number; and sending e-mails to recipients or recipient lists.
The ISMS shall allow the implementation of SOPs for, at least, the following scenarios:
▪ Alarm Video Verification
▪ Routine Video Guard Tours (allowing multiple checkpoints)
▪ Entry and Exit Management:
▪ Remote Intercom Attendance
▪ Access Control Exception Handling (like card error, access denied, etc.)
▪ Escorting People or Vehicles
▪ Emergency Situations (earthquake, fire, explosion, acts of terrorism,

riots, evacuation, etc.)
▪ Security & Safety Technical Issues
▪ Other custom SOPs for "On-Demand" Alarms (to be manually generated by the SDMS operators)

Workflow Customization
The ISMS shall allow for complete customization of the workflows for each alarm or event, thus implementing the standard procedures of the organization.
The ISMS shall allow the configuration of different workflows for different alarm or event types. The workflows shall be configurable per site, i.e., allowing different workflows for different sites (for example, evacuation procedures could be different from building A to building B).
The ISMS shall allow for global templates, i.e., global standard procedures for given alarm or event types that can easily be imported into one or more remote sites. In this way, when a change must be made to an SOP, it will be enough to change the procedure's global template, and that change will immediately propagate to all the sites configured with that procedure.
Simplicity
The ISMS shall be simple to learn and to operate it shall offer the operators a "clean" interface, avoiding unnecessary buttons, menus and windows.
A new operator shall be capable of immediately recognizing the anchor areas of the ISMS: the Alarms Queue and the Map. After picking an alarm or event, the operator should immediately view the workflow with the instructions to follow. This will cut down on training times and prevent security gaps that typically occur due to long operator learning times.
The ISMS shall also avoid other pitfalls of typical PSIM[2] software in terms of complexity and setup times, because this will severely limit the number of certified system integrators capable of installing the ISMS
The ISMS manufacturer shall be capable of fully training an installer, in installing, configuring and maintaining the SDMS, in one week or less.
Alarms Queue
In the ISMS Alarms Queue all active (in progress) alarms or events shall be listed in descending priority. Alarms shall be listed and aggregated (clustered) by site, with each row in the queue being associated with a given site.
Sites shall be identified by their names and locations. When a site has more than one active alarm, the icons for the active alarms are listed in the bottom of each row.
Alarm icons shall indicate both the type and priority of the alarm or event. A red background in the alarm icon shall mean “critical”, a yellow one shall mean “high priority”, a green one shall mean “medium priority” and a blue one shall mean "low priority".
The operators shall be able to manually add new "on-demand" alarms by clicking a button that should be next to the Alarms Queue for convenience.
Workspace
The ISMS Workspace shall be a task-oriented area. The operators shall easily and quickly store open or pending tasks for later use, i.e., situations that still require attention or further action.

The operators shall be able to minimize an open task to the Workspace, leaving it aside for a while, in order to handle a new situation. Each operator shall have a distinct Workspace and shall not see or change the Workspace of other operators.
The Workspace area shall be filtrable to only show the selected types of pending tasks.
Map
In the ISMS Map area, the operators shall get a geographical view of the entire area or region covered by the ISMS. The ISMS Map shall open with the zoom level adequate to show all the remote sites being managed by the ISMS.
Remote sites shall be shown in the Map, and whenever there are pending alarms or events at that site, the corresponding alarm icons shall indicate that situation by appearing over the site icon. The operators can navigate the Map, "enter" a given remote site (see below "1.11 Navigation in Remote Site") or start handling an alarm or event that is active at a given site.
The operator shall be able to decide which information is shown on the Map: site labels, site icons, active alarms or events, and mobile devices (security equipment that sends its GPS position to the SDMS in case of alarm). To find sites and equipment, the operators shall be able to zoom in or out, or to use a "smart" search box that allows searches based on partial names.
The ISMS Map area shall allow the use of filters to quickly select a given site. The SDMS shall support "online" mapping services, like Google Maps, but also "offline" georeferenced maps like OpenStreetMap[3], if an Internet connection is not available or not authorized.
The ISMS shall allow toggling between map and satellite view. Depending on the zoom level, when there are sites very near each other, the ISMS Map shall be able to group neighboring sites in one icon with a different representation.
Floor plans
The ISMS shall allow schematic representations to scale of the sites to be monitored. These ISMS floor plans shall allow mapping the devices on its correspondent location.
It shall be possible to represent multiple devices as a group, combining related logical devices (that belong to the same physical device). This group of devices shall be identified with a different representation and should allow interaction with the entire group.
The ISMS floor plans shall have the option to be dynamic or static. If dynamic, when a new alarm or event is received by the ISMS, the correct floor plan shall be selected and centered on the location where the alarm or event was triggered.
The site floor plans shall allow defining device (or device group) influence areas, thus presenting the coverage areas for that device (or device group). These coverage areas shall be represented by different colors depending on the device (or device group) status.
Live Events
The SDMS should present a dashboard or list with real-time alarms and events that are being received. The SDMS Live Events dashboard or list should allow filtering based on alarm/event type, site, date/time and other.
Workflow

The ISMS Workflow shall be immediately shown to the operator when he/she selects an active/pending alarm from the Alarms Queue or from the Map. The Workflow shall flow dynamically according to the actions and answers of the operator: a next step shall depend on the action or answer that was given in a previous step.
The Workflow shall allow the operator to handle alarms or events step-by-step. ISMS workflows shall be easily configurable and changeable, using the ISMS configuration interface, without the need to recompile or add software modules to the ISMS.
ISMS shall support global workflows, i.e., SOP workflows that shall be used in several remote sites. In order to make the most of global workflows, the ISMS workflow configuration interface shall help the user in the task of customizing a global workflow template for a given site, by allowing the user to easily search for device IDs (of cameras, sensors, outputs, phone extensions, etc.) that must be added to, or changed in, the workflow.
ISMS shall allow for collaboration between operators: if an operator needs to leave a given workflow unfinished (to attend to a more important situation), the ISMS shall send the alarm back to the Alarms Queue after a given timeout in order to allow another operator to finish that workflow.
ISMS Reports shall indicate the operator that performed each and every task. Each workflow task shown in the ISMS Reports shall also contain a timestamp for each task completion.
At the end of the workflow, the ISMS shall display the following options: close the alarm; postpone the alarm (specifying a given delay); send the alarm to another operator group; and change the alarm type.
When closing the alarm handling workflow, theI ISMS shall allow for an optionally configurable alarm classification list to be shown to the operator, in order to ensure that alarms are being classified when needed. Alarm classification statistics shall be available within the Business Analytics module of ISMS.
When the operator tries to close an alarm without having completed the workflow, a mandatory non-empty comment box should be displayed in order for the operator to fill in the reason for the non-completion of the workflow.
At any moment during the workflow execution, the operator shall have access to the remote site resources (floor plans, device tree, site contacts, site alarms history and video search).
The operator, if allowed by group permissions, shall be able to add at any moment to the workflow: "live" snapshots, "live" video clips, recorded video clips, and any attachable file selected from the workstation's file system. The operator should also be able to add, at any moment, custom comments or remarks.

Alarm Video Verification
One of the goals of ISMS is to reduce false alarms and their costs via remote Alarm Video Verification. It is essential to detect a false alarm as soon as possible to avoid allocating unnecessary human resources to the false alarm. In the case of a true alarm, it is equally important to detect them as soon as possible to ensure a prompt response from the operators and from the security team.
An Alarm Video Verification workflow shall help the operator distinguish a false alarm (false positive) from a true alarm (true positive) by showing video & audio from the remote site ("live" and "pre-alarm" video); allowing phone calls to the remote site or to a supervisor; gathering detailed alarm and site information; and other actions.

Remote Guard Tours / Patrols

Remote Guard Tours or Patrols shall allow operators to complement, or replace, traditional on-site guard tours on foot by performing remote verifications. The ISMS shall guide the operator through a set of previously configured checkpoints.

Each checkpoint shall show the operator a set of cameras (from 1 to 4) in "live" together with a specific workflow for that checkpoint. At each checkpoint, the operator shall be able to see the "live" video feeds and will be guided in following the step-by-step instructions regarding information to collect; verifications to perform; or tasks to execute.

The ISMS shall store the operator answers and actions, together with any images, videos and comments that the operator may have added. The ISMS shall provide for the inclusion of this information in a report to be sent to a supervisor.

Remote Guard Tours should be configurable to be automatically triggered at specific dates and times, or at random times within a given time frame, but should also allow for manual triggering by the SDMS operator.

Entry and Exit Management

The ISMS shall help the operators in handling people and/or vehicle entry and exit situations that require human decision.

Within an ISMS workflow, the operator shall be able to receive intercom calls or access control exceptions to handle them; and, after validating the ID and the permissions of the person that wants to access the premises, decide whether to grant or deny access to employees, suppliers, visitors and security personnel.

When there is no access control system in the remote premises, the ISMS operator shall be able to use "live" video and audio from an IP intercom in order to perform remote identification and to remotely open doors and/or disarm intrusion systems or zones.

Navigation in Remote Sites

Navigation in remote sites is an important part of daily multi-site security operations: the ISMS operator shall check remote sites by accessing CCTV cameras, floor plans, alarm sensors, intercoms, phones and other site equipment.

The ISMS shall allow the creation and customization of an unlimited number of video mosaics, i.e., collections of cameras for "live" viewing from one or multiple sites. Each operator can have its own video mosaics that can be opened at any time in a single or multi-screen environment.

Reports

The ISMS shall allow the creation of custom reports with graphics (of alarm and/or event statistics) without having to export data to third-party applications to generate them. ISMS reports shall contain a detailed list of alarms and events with their date and time, the tasks or actions made by the operator when handling them, the operator comments and notes, images and video clips gathered by the operator, and two-way audio recording of VoIP calls made from the ISMS.

ISMS reports shall be stored in the Server and any user with the right credentials should be able to access them or send them by e-mail to one or more recipients.

ISMS reports should also be exportable to PDF format or to Microsoft Excel format. Video & Audio clips in the Reports should be exportable to a standard media format. All report creation and exporting operations should be auditable (see below "1.13 Auditing and Business Analytics").

The ISMS shall allow the configuration of scheduled reports: these reports, previously configured in terms of filtering criteria – site name, alarm types, etc. – shall be automatically created at the configured dates and times and sent to the configured email recipient(s).
Auditing and Business Analytics
The ISMS shall keep auditing records in its internal database of all the relevant operators' actions together with all the video & audio viewed by every operator when handling alarms or events. A user with the right privileges shall be able to access this action log in order to supervise and audit all the actions performed by all the users.
The ISMS shall make available to an authorized user a business analysis interface, in the form of an intuitive dashboard, that continuously shows the ISMS workload and the performance of the security team over time (last few hours): alarm priorities, alarm types, alarm response times and other relevant performance metrics.
Integration
The ISMS shall be an open platform, capable of integrating physical security and safety equipment like IP cameras, DVRs and NVRs, VMS, video wall decoders, alarm detection panels (intrusion, fire and CO) and receivers, access control systems, general-purpose I/O[4] modules, VoIP/SIP intercoms, VoIP/SIP Public Address, and GPS[5] devices into a single security management platform.
The ISMS shall integrate third-party equipment making use, when made available by the manufacturer, of the equipment's SDK or API This ensures that, if the manufacturer updates the equipment, while keeping unchanged the SDK or API, the SDMS will still be able to communicate with the updated equipment.
Standards
When the equipment to be integrated with the ISMS does not have an SDK or API or is not an alarm panel capable of being integrated through a gateway device, the ISMS shall also allow for an integration based on industry standards.
Operating via Ethernet link (TCP/IP network), the ISMS shall have generic drivers, based on industry standards, to allow the integration of third-party equipment that is compatible with those standards.
The ISMS shall offer generic ONVIF and RTSP drivers to interface with IP video systems; a generic ContactID driver and the possibility of establishing a SIP trunk with a VoIP PBX in order for the ISMS to interface with VoIP ("Voice-over-IP") equipment, like IP intercoms, VoIP Public Address system or any SIP phone extension.
Web
The ISMS shall be a Web application, operated via Web Browser (Google Chrome, Mozilla Firefox, etc.), to avoid the need to install client-side software in all the SDMS workstations.
The ISMS should be accessible via HTTPS[6] protocol, in order to have data encryption between the SDMS Clients and the SDMS Server.
The ISMS Client shall be HTML5 compliant. In this way, any ISMS user, from anywhere in the corporate network, with the right privileges and credentials, can access the Server via an HTML5-compliant Web browser.
APIs

The ISMS shall have a set of Application Programming Interfaces (APIs) supported by Web technologies to allow the integration of third-party systems or specific developments as a proprietary mobile application without having to rely on software developments from the ISMS manufacturer. The API shall have a set of well-defined interfaces/classes/objects allowing abstraction of the underlying implementation of the ISMS and interaction with its assets. The API should use RPC architecture to minimize the performance impact on the ISMS Server and on network latency due to the criticality of the system.

Floatable windows

The ISMS shall allow floatable windows in order to give more visibility and flexibility to the operators. Besides the workspace, the ISMS shall allow opening, in other monitors, of additional instances of relevant information such as maps, floor plans, site status, live events, and business analytics or video mosaics.

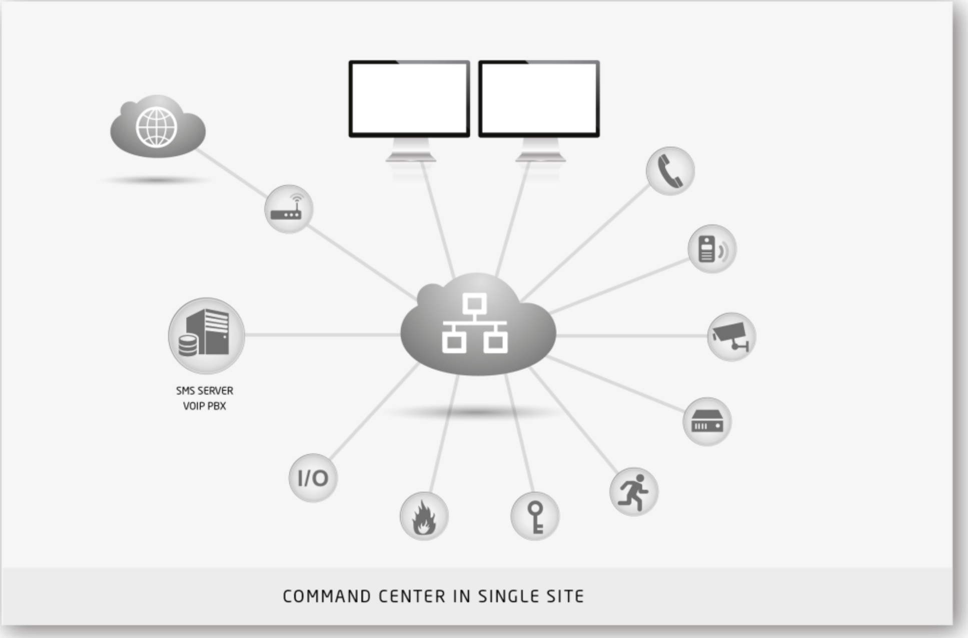
Video-wall

In order to provide more context to the operators and reduce the ISMS server load due to video requests, the ISMS shall be able to manage a video wall with contents fed either from IP decoders (with video from cameras, DVRs, NVRs or other), or from the SDMS server (as above in “1.18 Floatable windows”) or both. The SDMS video wall should support three types of monitors through the use of IP decoders:

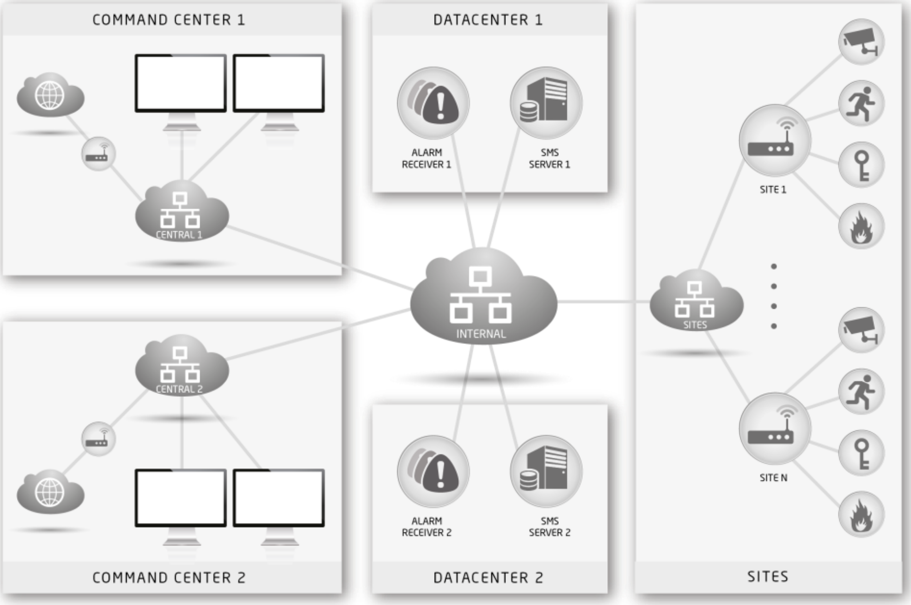
- **Mosaic monitor:** used to constantly monitor "live" video feeds from a site not associated to operation or to ongoing alarm handling;
- **Alarm monitor:** used to monitor an alarm, following its life cycle since it was triggered by showing "live" video feeds from cameras related with the alarm; these video feeds should be removed when the alarm is closed; the alarm monitor content should be automatically managed by the SDMS;
- **Operation monitor:** used as support for the operator, to see manually selected "live" video feeds, as an alternative to the SDMS web interface.

The ISMS manufacturer shall also provide its own decoder and still be capable of using third-party decoders.

ISMS Architecture



The ISMS single site architecture shall be based on a single Control Room where the ISMS operations team is located, and the ISMS server(s) and VoIP PBX are typically located in a datacenter. The Control Room can have multiple SDMS workstations where the SDMS is operated via Web browser.
The ISMS should also allow for multi-site architectures i.e., the use of SDMS to remotely supervise several places or buildings (sites) from one or more Control Rooms.



The ISMS architecture shall allow for several Control Rooms, or Command Centers, as well as fail over solutions, by having an ISMS Primary Server installed at Datacenter 1 and an SDMS Secondary Server installed at Datacenter 2.

Each Command Center shall have several ISMS Client workstations. It shall be possible for any ISMS workstation to have its own VoIP extension phone, whose extension number will be registered in the organization's PBX.

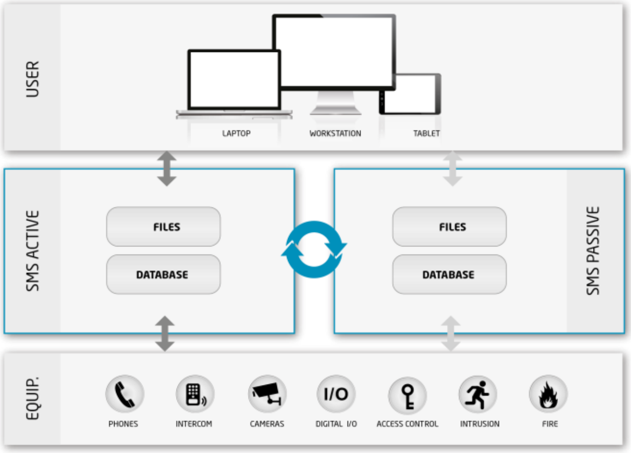
Whenever the ISMS operator needs to make a VoIP call from within ISMS, he or she shall be able to press a button in ISMS, typically within a particular workflow, in order to establish the connection between his/her workstation phone and the remote VoIP extension via SIP trunk with the PBX. All VoIP calls made from within ISMS shall be recorded by the SDMS Server.

Active / Passive Fail Over Architecture

It shall be possible to implement high availability (HA) clusters using an Active / Passive fail over architecture for ISMS. An Active / Passive HA implementation of ISMS shall comprise at least two server nodes, one for the SDMS Primary Server and another for the SDMS Secondary Server.

In normal ("Active") mode, the users access the ISMS Primary Server, which has its own database. Continuously, a synchronization process shall guarantee that the data in the ISMS Primary Server is the same as the data in the ISMS Secondary Server.

During this "Active" mode, the Web services of the ISMS Secondary Server shall not be running; only the database services shall be running to allow for data synchronization.



In case of failure of the ISMS Primary Server, it will be necessary to commute to the "Passive" operation mode. Commuting to "Passive" mode shall be done by a system Administrator, which will include starting the Web services of the ISMS Secondary Server.

Regarding media file management (audio and video files, and PDF reports), ISMS shall allow for two modes of implementation:

- Media file synchronization between the Primary and the Secondary ISMS servers (at each moment, there will be two copies of media data, one copy in each server);
- Unique media source, located outside of the ISMS Primary and Secondary Servers, in a network shared partition (at each moment, there will only be a copy of media data).

User Authentication

User authentication in ISMS shall be done through username and password. It shall be possible for an ISMS administrator-level user to reset another user password. It shall be possible to validate a given ISMS user against Microsoft Active Directory (AD) services using the LDAP protocol.

This integration of ISMS with AD via LDAP shall aim at authenticating the user's name and password, because the user’s permissions shall be configured and managed in ISMS; this means that ISMS does not need to import any permission or other user definitions configured in Microsoft Active Directory.

The communications channel between ISMS Server and Microsoft Active Directory services, to be protected by encryption, shall be established over SSL protocol.

13.

Standard Operating Procedures (SOPs)

One of the key features of ISMS shall be the possibility of configuring personalized SOPs according to corporate guidelines. ISMS shall allow an unlimited number of SOPs for on-demand situations (requested by the operator), as well as SOPs for each type of alarm or event that ISMS receives from the different systems it integrates.

Following, we give examples of **alarms**, **on-demand situations**, and **routine tours with CCTV cameras**; it shall be possible to handle these situations with ISMS, following standard step-by-step procedures:

Alarm SOPs (alarms generated automatically by the security equipment):

- CCTV: video loss, motion, etc.
- Fire Detection
- Intrusion Detection
- Access Control Exception (card error, out of schedule, access denied, etc.)

Emergency On-Demand SOPs (alarms generated manually by the ISMS operators):

- Fire
- Gas explosion
- Earthquake
- Bomb threat
- Terrorist attack
- Kidnapping
- Police patrol request
- Evacuation (any emergency requiring the immediate evacuation of a building)
- Post-emergency SOP (to return to normality after an emergency)

Other On-Demand SOPs (alarms generated manually by the ISMS operators):

- Lost persons or goods
- Cleaning request
- Maintenance request
- Technical problem
- Security guard request
- Flood
- Key delivery
- Key returning

Remote Tour SOPs with CCTV cameras (scheduled tasks to be performed by the ISMS operators):

- Perimeter

● Pedestrian entry points
● Vehicle entry points
● Supplier entry points
● Emergency exit doors
● Loading docks
● Technical areas
● Supervision of relevant visitor queues
● Supervision of relevant vehicle queues
Technical Requirements
Workstations
Because the ISMS shall be Web-based and operated via Web browser, the Workstations will only need a Web browser compatible with the ISMS, like, for example, Google Chrome or Mozilla Firefox, regardless of the operating system. The workstations should not require any additional installation besides the web browser.
Server Requirements
The ISMS Server shall run over Microsoft Windows Server, in order to allow for the installation of the third-party SDKs needed for SDMS to communicate with third-party equipment, because typically these SDKs are developed for Microsoft Windows.
The ISMS Server shall also be able to run over virtual machines with Microsoft Windows Server. The virtualization environment could be based on Microsoft HyperV or VMWare.

14. FOOTFALL SYSTEM *(One (1) Camera):*

The system to achieve the following metrics.
In/Out people counting.
Live occupancy.
Group counting.
Visit duration.
Queue counting.
Heat map.

People Counting Camera Specifications:

- Camera: 2x 5MP, 160°, RAM 1GB.
- Illumination: Minimum 1 lux.
- Frame Rate: 25 fps.
- Indicator: LED status indicator.
- IP Rating: IP64.
- Storage: Built-in, 8 GB Storage.
- Operating Environment: Temperature 10°C to 45°C, Humidity 10% to 90% Storage Environment Temperature -40°C to 70°C, Humidity 10% to 95%
- Tracking Technology: 3D-Spacing Mapping Video Tracking Technology and background removal on static objects.
- Field Upgradable: Manual / Auto Software upgrade

- Power Over Ethernet: IEEE802.3at.
- PoE Mode: Mode A/B.
- Cabling Cat5e/Cat6, 100Mbps.

BOQ/PRICE SCHEDULE

Item	Description	Qty	Unit Price (Kes).	Total Cost (Kes).
1.	**License Plate Recognition (LPR) System.**			
	License Plate Recognition Camera.	2		
	LPR System Software.	1		
	LPR System Monitoring Workstation.	1		
	Server.	1		
	Network Switch.	1		
	Cat 6A Network Cable (Roll)	4		
2.	**Command and Control Room.**			
	Industrial Monitor/Screen.	2		
	Air Conditioning Unit.	2		
	Security Door.	1		
	Network Cabinet.	1		
	High Back Orthopedic Chair.	4		
	Command Control Room Table.	1		
3.	**Radio Communication.**			
	Handheld Digital Radio.	6		
4.	**Key Management System.**			
	Supply and Install a Key Management System *(As specified in the tender document).*	1		
5.				
	Server.	1		
	Access Cards	500		
6.	**Traffic Arm Barrier.**			
	Supply and Install an Arm Barrier System *(As specified in the tender document).*	**1**		
7.	**Security Management (SMS) Software.**			
	Supply and Install a Security Management System Software *(As specified in the tender document).*	**1**		
	SMS System Monitoring Workstation.	**1**		
8.	**Footfall System *(People Counting System).***			
	Supply and Install a people counting system. *(As specified in the tender document).*	**1**		
9.	**Training & Commissioning:**			
	User Training for 30 Security personnel for 5 days.	20		

Total Cost:	
All Applicable Taxes:	
Grand Total:	

NB: Rates and Prices quoted should be net inclusive of all duties, taxes, levies, and insurances (where applicable) must be in Kenya Shillings or easily convertible currency.

Any pre-payment must be backed by a guarantee from a tier 1 bank or a security for a top 5 insurance company in Kenya.

Technical – (Scores - 70%)

Potential respondent to provide the following mandatory information.

I. **Company Profile:** Document detailing the company including its background, Products & services, clients, and expertise.

II. **Certification and Accreditation:** Detail any relevant certifications and accreditations by principals or accreditation bodies and attach copies of such certification. Such certifications may be for your company or for your individual staff as relevant to the work they do and the key skills for the service or goods you propose to supply. Manufacturer's Authorization and warranty.

III. **References**: Please provide in the table below details of at least Five (3) projects you have undertaken relevant to the job you are bidding for and performed over the last three (3) years, or that are relevant to this prequalification document.

IV. Two Years Audited Financial Statements Proposed Work Plan (Work Method & installation Schedule).

4 FORMAT OF RESPONSE TO TENDER

4.0 Information to be provided by bidders.

All bids should contain **ALL INFORMATION REQUESTED IN SECTIONS 4.** The information should be in the following order.

4.1 General Information about the firm

Provide the following documentation in respect of your company.

(i) **Certificate of registration** (or its equivalent) that is valid in accordance with any legally recognised jurisdiction.
(ii) **Tax compliance certificate** (or its equivalent) that is valid in accordance with any legally recognised jurisdiction.
(iii)Current County **Trade license/Business permit**
(iv)**Accreditations** or a licence where applicable

(v) **Company Profile**, with a clear **organogram** and area of speciality

(vi)List of **Directors** (Name, ID Number/passport number, Nationality, Telephone and physical address

(vii) Britam **Non-Disclosure Agreement** (document to be provided to accompany this RFP)

(viii) Britam **Supplier Code of Conduct** (document to be provided to accompany this RFP)

(ix)Britam Business Litigation and Probity; and Lead Time and Credit Period Declaration Form (document to be provided to accompany this RFP).

4.2 Bid Preparation and Submission

Bid documents should be in PDF format. Password Protected.

RFP FOR SUPPLY, INSTALLATION, TESTING, COMMISSIONING AND MAINTENANCE OF SECURITY EQUIPMENT AT BRITAM CENTRE

All Tenders may also be posted/ delivered earlier than the deadline to the below email:

tenders@britam.com

with a clear subject line *"RFP FOR SUPPLY, INSTALLATION, TESTING, COMMISSIONING AND MAINTENANCE OF SECURITY EQUIPMENT AT BRITAM CENTRE"*

Offers must be submitted in two separate documents, 1(one) technical- and 1 (one) commercial bid, **password protected** and clearly identified as:

- The file with the technical proposal should be identified as follows:

NAME OF THE COMPANY, TECHNICAL PROPOSAL FOR SUPPLY, INSTALLATION, TESTING, COMMISSIONING AND MAINTENANCE OF SECURITY EQUIPMENT AT BRITAM CENTRE

The file with commercial proposal should be identified as follows:

NAME OF THE COMPANY, COMMERCIAL / FINANCIAL PROPOSAL

5 GENERAL CONDITIONS OF CONTRACT

5.1. Introduction

Specific terms of contract shall be discussed with the bidder whose proposal will be accepted by the Company. The resulting contract shall include but not be limited to the general terms of contract as stated below from 5.2 to 5.14.

5.2. Award of Contract

Following the opening and evaluation of proposals, the Company will award the Contract to the successful bidder whose bid has been determined to be substantially responsive and has been determined as the best evaluated bid. Britam will communicate to the selected bidder its intention to finalize the draft conditions engagement in consultation with the bidder.

5.3. Application of General Conditions of Contract

These General Conditions (sections 5.2 to 5.14) shall apply to the extent that they are not superseded by provisions in other parts of the Contract that shall be signed.

5.4. Bid Validity Period

Bidders are requested to hold their proposals valid for ninety (90) days from the closing date for the submission.

5.5. Non-variation of Costs

The prices quoted for the service and subsequently agreed and into the contract shall be held fixed for the contract period.

5.6. Delays in the Bidder's Performance

5.6.1. Delivery and performance of the Transaction shall be made by the successful Bidder in accordance with the time schedule as per Agreement.

5.6.2. If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Services, the Bidder shall promptly notify the Company in writing of the fact of the delay, its likely duration, and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Company shall evaluate the situation and may at its discretion extend the Bidder's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.

5.6.3. Except in the case of "force majeure" as provided in Clause 5.14, a delay by the Bidder in the performance of its delivery obligations shall render the Bidder liable to the imposition of liquidated damages pursuant to Clause 5.7.

5.7. Liquidated damages for delay

The contract resulting out of this RFP shall incorporate suitable provisions for the payment of liquidated damages by the bidders in case of delays in performance of contract.

5.8. Governing Language

The Contract shall be written in the English Language. All correspondence and other documents pertaining to the Contract which are exchanged by the parties shall also be in English language.

5.9. Applicable Law

This agreement arising out of this RFP shall be governed by and construed in accordance with the laws of Kenya and the parties submit to the exclusive jurisdiction of the Kenyan Courts.

5.10. Successful Bidder's Obligations

The successful bidder:

5.10.1. Is obliged to work closely with Britam staff, act within its own authority, and abide by directives issued by the Company that are consistent with the terms of the Contract.

5.10.2. Will abide by the job safety measures and will indemnify the Company from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay all indemnities arising from such incidents and will not hold the Company responsible or obligated.

5.10.3. Will be responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanours.

5.10.4. Will not disclose the Company`s information it has access to, during the course of the work, to any other third parties without the prior written authorization of the Company. This clause shall survive the expiry or earlier termination of the contract.

6 BRITAM SUPPLIER CODE OF CONDUCT

6.1 GENERAL

This Code is applicable to all Britam suppliers (hereinafter "Supplier" or "Suppliers") and their employees (be they temporary, casual, or permanent) and sub-contractors throughout the world. Britam requires all Suppliers to conduct their business dealings with Britam in compliance with this Code and in compliance with all laws applicable to the Supplier's' business, wherever conducted. By entering business transactions with Britam, the Supplier agrees to abide by the terms of this Code and acknowledge that compliance with this Code is required to maintain the Supplier's status as a Britam Supplier. Britam shall have the right to terminate any Supplier's contract for failure to comply with the provisions of this Code. Britam recognizes that local laws may in some instances be less restrictive than the provisions of this Code. In such instances Suppliers are expected to comply with the Code. If local laws are more restrictive than the Code, then Suppliers are expected to comply with applicable local laws.

6.2 PROVISIONS

Suppliers must comply with the following:

6.2.1 Relations with competitors

Suppliers will be required to comply with applicable antitrust or competition laws and will not engage in any restrictive trade practices. Suppliers will always act in a manner that will uphold and encourage healthy competition.

6.2.2 Bribes, Conflicts of Interest, Gifts, and other Courtesies

6.2.2.1 Bribes

Suppliers shall not make or offer bribes or payments of money or anything of value to any Britam employee or any other person including officials, employees, or representatives of any government or public or international organisation, or to any other third party for the purpose of obtaining or retaining business with Britam. For the avoidance of doubt Britam considers an act of bribery to include the giving of money or anything of value to anyone where there is belief that it will be passed on to a government official or Britam employee for this purpose. Suppliers are required to comply with all applicable local anti-bribery laws.

6.2.2.2 *Gifts and other business courtesies*

Suppliers shall ensure that any expenditure incurred in relation to any Britam employee or government official is in the ordinary and proper course of business and cannot reasonably be construed as a bribe or so as to secure unfair preferential treatment. A general guideline for evaluating whether a business courtesy is appropriate is whether public disclosure would be embarrassing to the Supplier or Britam.

Britam employees may accept unsolicited gifts from Suppliers provided:

- they are items of nominal value – Kes1500 or less, or
- they are advertising or promotional materials having wide distribution e.g., calendars, stationaries, diaries, etc.; and
- Acceptance of the gift does not violate any applicable law.

6.2.2.3 *Conflicts of Interest*

No supplier shall enter a financial or any other relationship with a Britam employee that creates a conflict of interest for Britam. A conflict of interest arises when the material personal interests of the Britam employee are inconsistent with the responsibilities of his/her position with the company. All such conflicts must be disclosed and approval to the transaction given.

6.2.3 Compliance and implementation

6.2.3.1 Licenses and Returns

The Supplier will be required to obtain and renew, in accordance with any law or regulations all permits, licenses and authorizations required for it to carry out its business. In addition, the Supplier will be required to prepare and file any returns that it may be required to file under its incorporation statute, the Companies Act.

6.2.3.2 Taxation, Financial Integrity, and Retention of Records

- The Supplier will comply with all revenue laws and will not evade tax.
- Suppliers will be required to maintain accurate and reliable financial and business records and shall not have any false or inaccurate accounting books or records related to Britam for any reason. Suppliers shall maintain all business records at the minimum in compliance with the provisions outlined by the Kenya Revenue Authority or local revenue authorities from time to time.
- When any government investigation or audit is pending or ongoing then Suppliers will not destroy any relevant records until the matter has been investigated and closed.

6.2.4 Violations

If a Supplier becomes aware of any known or suspected improper behaviour by another Supplier in relation to their dealings with Britam or if a bribe or other inducement is requested from a Supplier by any Britam employee or any other person with the promise of influencing Britam's position as far as that Supplier is concerned or if the Supplier feels that a conflict of interests exists with one of Britam's employees then all pertinent details should be reported in confidence to the following Contact Address

Procurement procurement@britam.com

6.2.5 Variations

Britam reserves the right to vary this Code at any time.