

Terms of Reference and Design Brief - Design and Build of a Primary Data Centre in Sierra Leone

RFP Ref No: 2021/25266

1. Background and Justification

A Civil Registration system is the bedrock in building democratic institutions by providing credible and accurate legal identity evidence of citizens. Democratic, government and non-government institutions engaged in support and service provisions in the area of human rights, such as, child, gender, disadvantaged population groups, education and social welfare rights, etc. need evidence of facts of birth, death, marriage and divorce legal documentations of citizens on a continuous and permanent basis.

The Government of Sierra Leone developed an ambitious policy in 2014 to reform civil registration in the country and to establish a national identity register system. The 2014 National Civil Registration Reform Policy, as a goal, foresees the establishment of an integrated, continuous, and permanent national civil registration, vital statistics and identity registry system and provides clear policy directives regarding the governance and infrastructure transformation requirements.

It is against this background and policy directives of the Government of Sierra Leone that the European Union in 2017 committed 11,000,000 EUR to support the establishment of an effective Civil Registration system as a key priority under the EU programme to support democracy and governance in Sierra Leone.

Under the Financing Agreement SL/FED/038-586 for support to the governance sector in Sierra Leone signed on 19th October 2017 between the European Union and the Government of Sierra Leone, the EU committed to support the establishment of an integrated, continuous, and permanent national civil registration, vital statistics, and identity registry system in line with the 2014 National Civil Registration reform policy and 2016 NCR Act.

The EU contribution aimed at strengthening the Civil Registration system, in synergy with EU support to education, elections and public sector reform fields, and contributing to the following key expected results:

1. Sierra Leone's current birth and death registration rates are increased through citizen access to civil register service centres and document extracts.
2. Priority institutions have continuous, real-time, synchronised access privilege to and notification from the national database and have capacity to extract vital statistics.
3. High quality connectivity between priority agency databases and the central civil registry database established. Database is procured and customised. Software is installed and functional. Technological equipment for remote data delivery to the central database is available.

Hence, the EU funded support to the National Civil Registration Authority (NCRA) shall help maintain a permanent, continuous, decentralised, and universal registration of vital events (such as birth, marriage, death) across the country, accessible to households and individuals. Real-time data access to an

interoperable civil registration database shall allow a broad range of relevant state institutions to carry out their mandates, improve information-based decision making and service delivery.

2. Overall Objective - Primary Data Center

Technology will facilitate many of the key concepts of the Civil Registration Act, by enabling direct electronic registration of vital events to an integrated and interoperable civil registration database wherever it is possible in addition to the traditional paper-based system that will be conducted at the local CR offices permanently established in the chiefdoms and sub-cities. This registration data can be uploaded periodically in the system through the district offices. The backbone of this system has 2 main elements:

1. ICT and power supply solutions for the Primary Data Centre (at new NCRA HQ) - includes the server room, servers, storage, communication equipment, UPS, etc. Also, associated works to “fit out” the server room, with raised floor, false ceiling, environmental controls (AC), fire suppression systems, access control, etc. An automated backup power system (generator) is also included as a standalone solution to provide instantaneous power supply to ensure the uptime of the Data Center only. The Primary Data Centre (PDC) shall be Tier III compliant.
2. Customised Civil Registration & Vital Statistics (CRVS) Software - The proposed version includes functionality to record Vital Events such as births, deaths, and marriages, plus the registration of other vital events such as divorce, adoptions, etc. Additionally the system will enable backlog registration, personal data update, printing of certificates, etc. The software ensures the interoperability with other systems in other Ministry Development Agencies (MDAs) and the respect of all applicable national and Global Data Protection rules.

3. Immediate Objectives:

The contract includes the Design and Build of the Server Room that will house the Primary Data Center (PDC) and a smaller room to house the UPS and batteries. The Contract also includes the equipping, commissioning, and testing of the Server Room and PDC prior to the installation of the CRVS software.

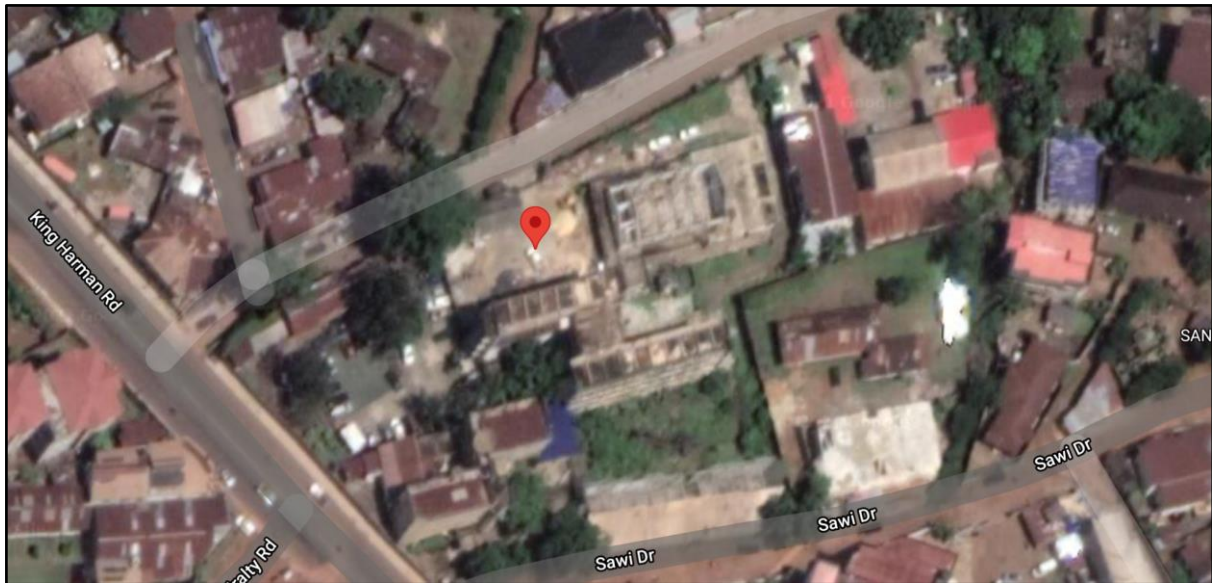
3.1 Site Data:

The Primary Data Centre (PDC) will be located at the new NCRA headquarters which will be located at the following location in Freetown, Sierra Leone:

National Civil Registration Authority
26B Off King Harman Road,
Brookfields
Freetown
Sierra Leone.

GPS: 8.471302, -13.246172

<https://www.google.com/maps/place/8°28'16.7°22N+13°14'46.2°22W/@8.4710001,-13.2462486,17.07z/data=!4m5!3m4!1s0x0:0x0!8m2!3d8.471302!4d-13.246172>



Satellite image of the NCRA HQ

The NCRA HQ is currently under renovation with the works expected to be finished by September 2021. The building is a 4 storey (Ground floor, first floor, second floor and Third floor) concrete structure (see picture below).



NCRA HQ (under renovation)

The Primary Data Center will be located on the 2nd floor. The Server Room, which is currently under renovation, has the approximate dimensions of 8.75m x 4.70m (28'-8" x 15'-5"). The expected height from finished floor to ceiling is 2.72m (8'-11"). There is a structural beam that is 0.27m (10.5") deep from ceiling height. See photos below:



Server Room view to right hand side.

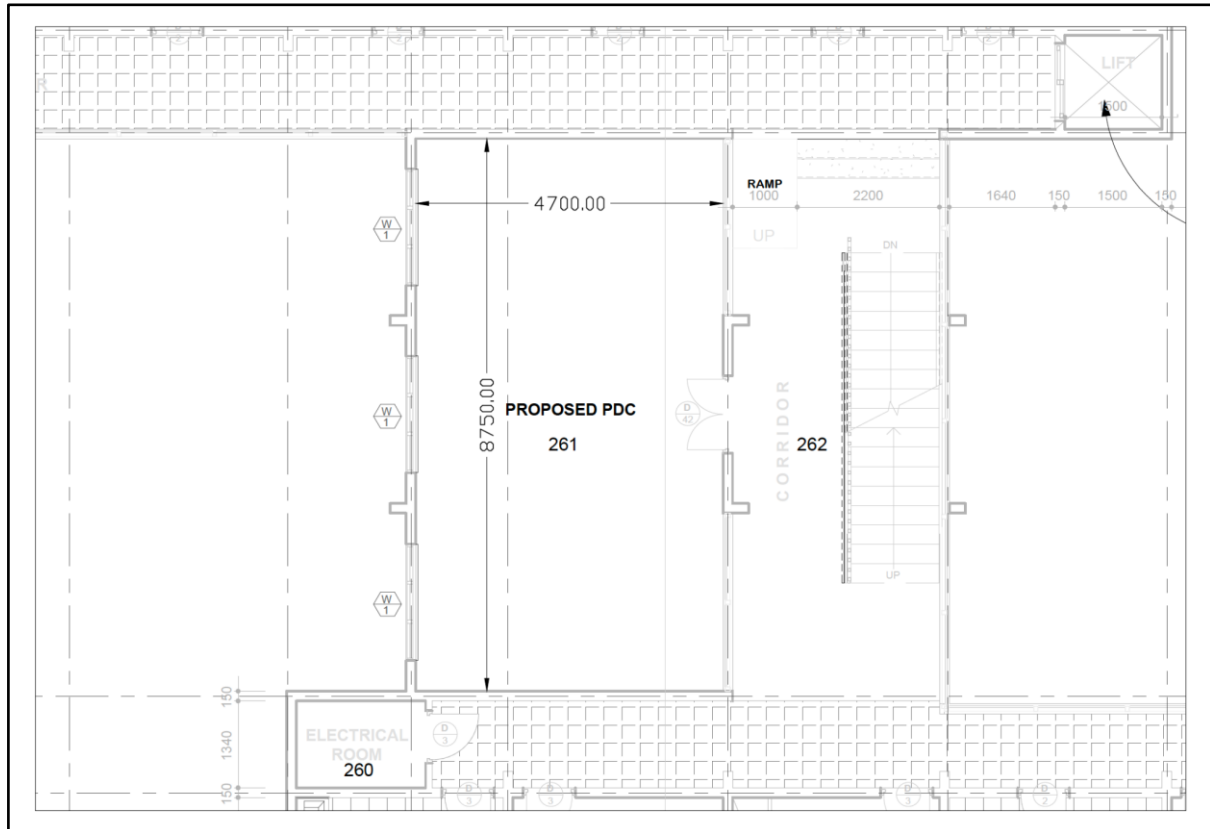


Server Room view to left hand side.

Note: The current windows will be blocked up during the renovations.

3.2 Drawings

The proposed PDC Server Room can be seen in the following excerpt from the drawings. The room is numbered room 261 and labelled “Proposed PDC”. The batteries for the UPS will be housed on the ground floor, as shown in the drawings attached separately to the RFP provided for Informational Purposes Only.



Server Room in new NCRA HQ.

A full set of AutoCAD drawings of the NCRA building are provided separately to the tender package for Informational Purposes Only. The Contractor shall be responsible for verifying and interpreting all Site Data and undertaking any such further independent tests or investigations that it deems required in order to establish the veracity of the Site Data.

3.3 Primary Data Center Philosophy

The NCRA is committed to establish new Data Centers compliant with Tier-III standards with business continuity mechanisms.

A Tier III Data Centre is concurrently maintainable with redundant components as a key differentiator, with redundant distribution paths to serve the critical environment. Tier III is described as “CONCURRENTLY MAINTAINABLE” and ensures that ANY component can be taken out of service without affecting production. Tier III Data Centre architecture should provide 99.982% availability (1.6 hours of downtime annually).

4. The Assignment:

The assignment comprises of 3 components:

Component 1: Server Room Design

Pre-design study: upon mobilization, the contractor shall perform a pre-design study to confirm the specifications of the various Server Room systems, namely the Environmental Control system, Fire Suppression system, UPS (housed separately) and Backup power supply generators, etc. to ensure that they are suitable for the requirements of the Primary Data Center.

The outputs of this study will be a design brief report which will be submitted for UNOPS approval prior to commencing the design phase.

The pre-design study shall include the review of specifications included in the Employers Requirements, calculations to determine suitability of all systems and components that comprise the server room (excluding the PDC).

Server Room design: Following approval of the design brief report by UNOPS, the vendor / contractor shall commence the detailed design work of the server room, including all the required components, including but not limited to the raised floor, false ceilings, environmental controls, fire suppression system, Access controls, CCTV, UPS, and Automated Transfer Switch to the backup generator. The detailed designs shall include the following:

1. Detailed drawings of the Server Room, its components, design calculations and applicable codes / standards.
2. Bill of Quantities: this includes all items required to fulfil the scope of work and specifications of the Server Room and PDC.
3. Method Statement: a detailed breakdown of the plan the contractor / vendor choses to implement this assignment thus fulfilling the Employers Requirements. This should include details on the applicable codes / standards, team composition, construction schedule, quality control plans and Health and Safety, Social and Environmental management plans. Additionally, the development of a management plan to avoid or mitigate any adverse impact should be included.
4. Details of any Statutory Approvals required (if applicable) and which parties are responsible. The Schedule of Programme shall reflect these statutory requirements.
5. State derogations between the Employers Requirements, Design Brief and Final Design. All project derogations shall be agreed before submission to Design Review. Derogations may include Value Engineering and Innovation.

Design Review: UNOPS follows a defined design review process to ensure the quality of the outputs and services to meet international standards and regulatory requirements. The design review process is a mandatory requirement for the design of UNOPS infrastructure works, in order to mitigate organizational risk and ensure minimum standards of safety and functionality for partners and beneficiaries. This activity will be conducted by a third-party reviewer assigned by UNOPS when the full design of the Server Room and PDC is completed. The conclusion of the process will be marked by the issuance of the Certificate of Design Review Compliance by UNOPS. This certificate is required by UNOPS prior to proceeding to the construction of the Server Room and the installation of the PDC.

Approval Process: This process starts with the first design activity and continues throughout the entire design development work. The Contractor through this process will ensure that the design's outputs in the different stages meet the requirements of the beneficiary, the NCRA, and are approved in a timely manner. UNOPS will facilitate this process and coordinate with the relevant stakeholders as appropriate. The contractor who will conduct the design works should have appropriate experience in similar projects and is familiar with the approval process and its requirements.

Component 2: Server Room Construction

Installation: Upon the issuance of UNOPS design review certificate, the contractor / vendor will proceed with the installation of the Server Room in accordance with the approved design. The contractor is required to supply and install all the required components that comprise the Server Room, including but not limited to raised floor, false ceilings, environmental controls, fire suppression system, Access controls, CCTV, UPS, and Automated Transfer Switch to the backup generator etc. according to the Server Room specifications in Section 6: Specifications and Requirements of the Server Room. The installation shall be executed and monitored according to the method of statement prepared by the contractor, and progress approved by UNOPS. The contractor shall be responsible to make available during the construction period suitably qualified technical staff to manage construction and to respond promptly and efficiently to technical queries relating to the design and specification of the project.

Commissioning, testing and inspection: Upon completion of the installation of the Server Room and prior to the installation of the Primary Data Center, the Contractor shall perform the necessary actions to commission and test all systems of the Server Room. A joint inspection of the completed Server Room shall be conducted by the Contractor, UNOPS and any other qualified parties at the request of UNOPS. Upon successful completion of the commissioning and testing, the Contractor shall request in writing permission to proceed with the installation of the Primary Data Center.

Component 3: Primary Data Center Installation

Installation: The contractor is required to supply and install all the required IT components that comprise the Primary Data Center, including but not limited to servers, switches, racks, backup drives, UPS etc. according to the PDC specifications in Section 7: Specifications and Requirements of the Primary Data Center. The contractor shall be responsible to make available during the installation period suitably qualified technical staff to manage the installation and to respond promptly and efficiently to technical queries relating to the design and specification of the project

Commissioning, testing and handover: Upon completion of the installation of the Primary Data Center the Contractor shall perform the necessary actions to commission and test all components of the PDC. A joint inspection of the completed Primary Data Center shall be conducted by the Contractor, UNOPS and any other qualified parties at the request of UNOPS. The contractor will provide UNOPS with a full set of "as-built" drawings for the Server Room and Primary data Center connection upon completion.

After completion of the installation, commissioning and testing of the Primary Data Center the Contractor shall request the "Taking over Certificate" to formalise the handover of the completed works to UNOPS. UNOPS will conduct a formal joint inspection of the works with the Contractor and NCRA

to verify that the Works are “Substantially Complete”. The NCRA will acknowledge that the works are substantially completed, and the PDC is ready for operation by the NCRA and is under their full control. Upon acceptance of the Substantial Completion of the Works, UNOPS will issue the “Taking Over Certificate” to the Contractor. The date of issuing this certificate will also be the commencement date of the 12-month Defect Notification Period (DNP) as defined within the Contract.

At the end of the 12-month DNP, UNOPS will conduct another round of inspections of the PDC and once satisfied that the Contractor has fulfilled the Performance of the Contractors Obligations, UNOPS shall issue the “Final Completion Certificate”. Simultaneously, UNOPS shall formally conduct a final handover to the NCRA with the issuance of the Final Handover Certificate. By signing the Final Handover Certificate, the NCRA acknowledges and accepts that Contractors’ Obligations under the contract have been completed to a stage ready for the Final Completion Certificate to be issued by UNOPS and that the DNP has expired.

Schedule of Programme

The work should be delivered per Activities according to the milestones table below. Each period indicated is envisioned from commencement to completion of the works. The period starts when a commencement order is issued by UNOPS for each activity.

Activity #	Area of Works	Period
Activity One	Pre-design Study - Design Brief	Two Calendar Weeks
Activity Two	UNOPS approval	One Calendar Week
Activity Three	Detailed Design for PDC	Two Calendar Weeks
Activity Four	Design Review and DR Certificate issuance by UNOPS	Three Calendar Weeks
Activity Five	Installation of the Server Room - Works - Commissioning and Testing	Four Calendar Weeks
Activity Six	UNOPS approval	One Calendar Week
Activity Seven	Installation of the Primary Data Center - Commissioning and Testing	Four Calendar Weeks
Activity Eight	Training and delivery of O&M Manual	One Calendar Week
Activity Nine	Defect Notification Period	12 Months

5. Deliverables

The Deliverables for this contract can be summarized by the following:

5.1. Design Brief

The preparation of the design brief, in consultation with stakeholders, should serve to identify user requirements, relevant codes and standards, breakdown of construction costs and quality expectations.

Relevant codes, standards, and minimum requirements must be clearly identified, site investigations, and environmental and risk assessments should be carried out in preparation of the design brief.

It must be emphasized that the brief should always be reviewed and approved by UNOPS before further design work is initiated. This is to ensure that the brief accurately represents the scope of the works and to prevent any changes to the scope without a corresponding adjustment to the agreed budget and timelines.

The design brief documentation should include:

1. A full description of the scope of works.
2. Site information based on site investigations and surveys.
3. Conceptual design and technical design calculations / assumptions.
4. Provisional Bill of Quantities (BoQ) with estimated construction costs.
5. Proposed codes and standards to be used in the design. Any other national or international requirements.
6. Proposed Schedule of Programme
7. Any specific design considerations, such as material choice, compatibility with existing built environment.

5.2. Final Design

The final design must include the following documentation in line with UNOPS Design Review expectations:

1. **Design report.** It provides a background to the development of the design, and a concise synopsis of the design issues and the design philosophy applied, including information on user requirements, site surveys, and relevant codes and standards.
2. **Design Documents.** At the final design stage, drawings must be sufficiently detailed and informative to build the Server Room and Primary Data Center to the performance requirements. It will be necessary to include the following:
 - Location plans / site information
 - Server Room design, including all calculations for ancillary equipment (including, but not limited to the Environmental Control System, Fire Detection and Suppression System, UPS System and Backup power supply, etc.)
 - Primary Data Center design (demonstrating Tier III compliance)
 - Drawings and details of all external connections / equipment. i.e. AC compressors, Backup generators etc., including details of the secured compounds.
 - Final Bill of Quantities (BoQ) with detailed construction costs.

- Final Schedule of Programme.
- Signage plans.
- Health and Safety Management Plan
- Environmental and Social Impact Assessment
- Other necessary documentation related to specific type of works.

The design documents have to be issued to the following standards:

- a) Designs. All drawings shall be prepared to ISO and UNOPS drawing standards (to be provided by UNOPS to the successful vendor). They shall include all layouts, sections, details, dimensions...etc. Drawings shall include.
 1. Full title blocks including the name and logo of the NCRA, EU (donor) and UNOPS.
 2. Drawing numbers
 3. Revision numbers
 4. Revision details
 5. Legends
 6. Scale
 - b) Full set of drawings. Drawings shall consist of the following types of sheets in the order listed.
 1. Cover Sheet
 2. Index Sheet (if necessary)
 3. Standard general Notes and Notes
 4. Plan Sheets
 5. Details Sheets
 6. Standard Sheets and Special Details.
 - c) Full set of drawings is required to be reviewed by UNOPS before issuing for approval, price includes submitting 2 two hard copies on A1 paper size (or suitable for scale of sheets) for the full set of construction drawings per each revision, accompanied with the PDF and AutoCAD (DWG) soft copies, named, and classified as per approved filing system for reviewing by UNOPS.
 - d) Full set of drawings is required. Submitting 6 six hard copies on A1 paper size (or suitable for scale of sheet) for the full set of approved design drawings per each revision. And a full set of drawings soft copies with PDF and AutoCAD format.
 - e) All documents and drawings should be arranged, named, and classified using a standard best practice filing system. This will be approved by UNOPS prior to use.
 - f) The contractor should make any necessary visits to the project site to integrate full coordination with other onsite contractors and UNOPS Engineers for the design requirements, reviewing and in addition to follow up any further technical queries during construction.
3. **Technical specifications & schedules.** Detailed specifications and any associated schedules specify the requirements of the proposed materials, products or services incorporating any special provisions and constraints. Technical specifications shall be provided with a full description of work for every BoQ work activity. All relevant standards, manuals, and guides should be cited, as these will be used as the basis for quality assurance, control, and payment for completed works.

4. **Engineering calculations** the source and the basis for formulas, figures and reference used in the calculation process shall be provided and made easily understandable.
5. **Bill of Quantities (BoQ) with cost estimate for the construction works.** The BoQ shall include all relevant applicable work activities and quantities, description of work, material, methods of QA / QC measurement and basis of pricing.
6. **Method Statement.** A detailed breakdown of the plan the contractor / vendor choses to implement this assignment thus fulfilling the Employers Requirements. This should include details on the applicable codes / standards, team composition, construction schedule, quality control plans and Health and Safety, Social and Environmental management plans. Additionally, the development of a management plan to avoid or mitigate any adverse impact should be included.
7. **Statutory Approvals.** Details of any Statutory Approvals required (if applicable) and which parties are responsible. The Schedule of Programme shall reflect these statutory requirements.
8. **Derogations.** State derogations between the Employers Requirements, Design Brief and Final Design. All project derogations shall be agreed before submission to Design Review. Derogations may include Value Engineering and Innovation.

5.3. Operational & Maintenance Manual

To enhance the NCRA's capacity towards ensuring full and optimal use of the CRVS system in its totality and the smooth operation and maintaining of "uptime" of the Primary Data Center, the contractor will conduct a detailed and comprehensive training on the configuration and maintenance of the Server Room and PDC upon the completion of all related works. Additionally, and to ensure that such knowledge is maintained, an operational and maintenance manual will be prepared by the contractor and provided to the NCRA. The manual will contain information and strategies designed to guide users on the proper use of the Server Room and PDC and its ongoing maintenance and routine upgrades. It will also contain detailed information on the control requirements, scheduling information and operating procedures necessary to successfully operate such a Server Room and its systems. In essence, the operational manual will provide IT and maintenance personnel with the information necessary to maintain the Server Room and PDC effectively.

5.4. Reporting / Monthly Design reports

The monthly progress reports will detail project status related to progress against the schedule, potential delays, and recommended course of actions; outstanding issues from the previous month and remedial actions undertaken; and planned activities for the coming month.

9. Specifications and Requirements of the Server Room.

9.1. Server Room Requirements

Location:

NCRA Building – Freetown Sierra Leone. See above section 3.1

9.2. Walls, Ceiling, Fire Resistant Doors and Ramp

Room walls, ceiling, and doors should be sound isolated from other occupied areas. A false Ceiling is not necessarily needed; however the contractor should provide a suitable and adequate sound insulation, whilst maintaining sufficient headroom and clearance for server racks, cooling, and all installed equipment in the Server Room.

Antistatic floor finishing (no wax) is recommended for raised floor tiles or sheet vinyl.

The Supplier should install 1 (one) wide access door (1400mm x 2100mm) with the following characteristics:

- Fire resistant 60 minutes, equipped with electromagnetic locks and reset mechanisms.
- In the event of a power loss, the door will be capable of opening from inside without the use of key cards or power.
- minimum thickness 45mm, with frame and fire rated vision panel, SS ball bearing butt hinges, SS lever with internal thumb turn and external key operation with heavy duty door closer, (panic bar and door frame bottom threshold to prevent leakage of conditioned air) etc. all complete to be operated with Access Control.

For easy access to the room with heavy equipment and infrastructure items, an access ramp of efficient inclination will be constructed such that equipment on trolleys or on wheels may be easily moved to/from the Server Room.

9.3. Physical Security Specifications

9.3.1. Access Control System (Quantity 1)

For security reasons and protection and safety of sensitive data, a physical access control system should be installed in the new Server Room, so only “Authorized Persons Only” can physically have access.

The system should provide the possibility of programming the necessary number of access levels and time schedules to manage the physical access of different groups of cardholders to every secured area.

Entry to the server room will require PIN or individualized card or **(PIN and Card)** to control access. Every card entry and personnel will be logged at the security station.

It should offer the possibility of expansion of sites via TCP/IP (LAN/WAN), directly to the network-ready door controller unit. The door controller should have the capability of controlling up to 4 card readers

for 2 and 4 door configurations, with integrated PIN keypad for extended security and prevention of lost and stolen cards to access the secure area.

The functionality of the access system should not be compromised in case of lost connectivity with software and when connection restored should download all the events buffered in the internal non-volatile memory.

The controller should be provided with an internal battery with full functionality for up to 12 hours in case of AC power failure.

The controller board should be installed in a lockable metal cabinet with Tampered Supervision (internal tamper detection device that signals when the cover is removed, preventing an intruder from switching down the system or removing controller board completely) to be provided by the supplier.

Required build in ports for the controller:

- 1x10/100 Base-T for server connection,
- 1xRS232 for alarm panel integration,
- 1xRS485 for future door expansions.

The controller should comply with EN61000-6-1, EN61000-6-2, EN55022, EN60950, FCC Class A, UL-294, UL-1076, RoHS, and CE.

The card reader technology should be within proximity of a 125 kHz transponder with not less than 39 bits of encryption for extended security and risk of card duplication, with reading distance not less than 15 cm, and with built-in bi-colour LED lights.

An electromagnetic lock with bond sensor, shall be installed on the access door, with a contact sensor for continuous door state supervision. The electromagnetic lock with bond sensor shall have an LED (locked/unlocked/not properly locked) status display and a minimum holding force 272 kg (600 lb.).

Also, one hydraulic door closer should be mounted for automatic closing of the door.

In the event of a power failure or other serious fault condition (e.g. fire, release of the fire suppression system etc.), the electric door lock will be fixed in the open position.

The door must be capable of manual override operation from the inside (so that persons may not be trapped inside the room, e.g. if there is a fire or release of the fire suppression system).

A set of 50 RFID cards should be supplied.

9.3.2. IP Camera Based Surveillance and Motion Detection System (Quantity 1)

For complete monitoring of protected areas, the installation of an IP Camera based surveillance and motion detection system is required. The system has to be built based on an IP solution to provide management and recording from one or more remote sites.

The Network Video Recorder (NVR) will be placed in the Server Room and should make possible monitoring and recording of IP cameras on site through the LAN network of the Server Room.

The CCTV should be physically separated from the Data Centre Infrastructure LAN network. This can be realised by separating these networks physically or by implementing VLANs.

NVR System should enable 6 months of recording at the camera settings: 5 MPix, MPEG4 compression, frame rate (fps) 60. NVR must have the memory for the video content recording of at least 10 TB capacity.

Software system should have provision for change / motion detection.

The system should provide high quality video images in live view mode and in recording mode.

The NVR should be capable of supporting future camera extensions on the same system.

All camera recordings shall have Camera ID & location/area of recording as well as date/time stamp. Camera ID, Location/Area of recording & date/time shall be programmable by the system administrator with User ID & Password.

The CCTV system shall cover the corridor, power generator location and main entrances with IP cameras.

The server room should be covered with a minimum of four IP cameras, whilst the UPS battery room should be covered by at least 2 cameras. Camera resolution must be at least 5 MPixels.

Cameras must be accessible through the mobile app.

For the stability of the CCTV system, the MTBF declared from the manufacturer not less than 35,000 hours.

9.4. Raised Floor (Quantity 1)

Fixing steel raised access floor of FFH at least 400mm, finished with antistatic high-pressure laminate in size 600 x 600 mm x 35 mm with point load 450 kg and uniform distribution load (UDL) 1350 kg per square meter.

All Electrical and Data Raceways should be installed under the raised access floor supplying installed 19" Racks

The design should be made for minimum 12 x 19-inch 42U Racks

The pedestals should support various elevations from the floor.

Raised Floor shall be Fire resistant according to DIN 4102-2 F60, 61dB sound reduction and 1500.

The raised floor must be properly grounded. Also, the pedestals to support the elevation from the floor will be installed.

The entry ramp shall also be installed.

Also, a Metallic raised floor grates, Size 598 x 598 x 40 mm (WxLxH), Free cross-section 88%, Max. Surface load 50,000 N/m² with even distribution Max. Point load (on 200 x 200 mm area) 4,500 N shall be installed for each rack and UPS.

9.5. Environmental Control System (Cooling) (Quantity 1)

The environment inside the Server Room shall need to be continuously maintained at 21 C. The necessary alarms for variation in temperatures shall be monitored on a 24x7 basis and logged for providing reports.

The solution must come with the monitoring platform which is able to send SMS or email notifications.

Ambient RH levels shall need to be maintained at 50% ± 5 non-condensing.

Cooling System to provide constant temperature and humidity control in degrees C and the Relative Humidity (RH) based on the standards for active or passive components.

Humidity sensors shall be deployed.

The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.

The internal rack layout design shall follow the cold aisle and hot aisle concept.

Professional Air conditioning system, 74 KW with redundancy

- 2+1 Professional Cooling System, 74 KW total net sensitive cooling capacity (3 x 37 KW)
- Teamwork configuration of cooling units
7" Touch Display
All components integrated on a Modbus chain, including condensers
- System should modulate power based on actual heat load
- System should enable controlled communication with Cold Air Containment
- Unit shall have ModBus internal Modbus communication between all internal components, including condensing units
- IS-UNITY-DP - IntelliSlot Unity card with SNMP/Web, Modbus and BACnet communication card
Down flow, distribution of cold air under the raised floor
- Integrated ATS for dual power (Tier 3 requirement)

Taking into consideration that the system will be working 24 hours a day, 365 days a year, efficiency is a key consideration. These requirements should be fulfilled by digital scroll compressor and electronically controlled fan technology. No hot spots can be tolerated in the PDC.

Flexibility

Under the raised floor, airflow-cooling design is suitable for raised floors. Adjustable airflow (modulated cooling capacity and airflow) assures the proper cooling based on the actual needs of the IT dissipation.

Availability

Self-adapts to changing conditions to provide 24/7 precision environmental control: cooling, humidity control and air filtration. Precision cooling should control and provide alerts for preventive maintenance before issues occur.

Variable capacity Inverter Scroll compressor should adapt to the load and eliminate compressor cycling, greatly increasing compressor life.

Low Total Cost of Ownership

Precision cooling should be designed for higher return air temperature to maximize cooling capacity. Only front and back access required, resulting in minimized installation and service time. Inverter scroll compressor and variable speed fans should operate efficiently to reduce energy consumption.

Communication Card

Precision cooling should include the communication card IS-UNITY-DP - IntelliSlot Unity card with SNMP/Web, Modbus and BACnet.

The Web Card should deliver SNMP and HTTP web-management communications capabilities for monitoring and control through your existing network with no additional software required and allow remote monitoring and control of Precision Cooling using Web or your Building Management System.

Infrastructure equipment (UPS, HVAC, Genset, PDU, Fire Detection and Extinguishing System should be on a separate network with the monitoring system (application). Interconnection of the monitoring system with the LAN network of the agency (sending alarms, email, and access of monitoring clients to the server) shall be realised by a firewall.

By protecting the "Infrastructure Network" the HVAC, UPS and other equipment will be protected.

Inverter Scroll Compressor

The Inverter Scroll Compressor should use the latest control technology to deliver precise operation and significantly higher energy efficiency than other compressor technologies. In addition to the advantage of the dependable scroll design, Inverter Scroll technology should provide infinitely variable capacity modulation between 20-100% to enable the output to precisely match the changing cooling demands of the room.

Plug Fans

Plug fan technology should work to regulate airflow and reduce fan input power and deliver airflow for the optimal operating conditions for IT equipment.

Speed controllers on each motor should eliminate a single point of failure.

Modbus Controlled Cooling System Components

All components shall be integrated on a Modbus chain, including condensers. With Modbus controlled condenser units, the highest level of efficiency will be achieved

High Performance Air Filters should be easily accessed.

The cooling system should include condensers that support the above requirements.

The cooling units shall have integrated ATS.

Technical data:

Maximum net sensible cooling capacity - (*) kW	37,0
Minimum net sensible cooling capacity - (*) kW	11,8
Compressor modulation 80% (*)	
Nom. ESP Pa	20
Net Total Cooling Capacity kW	31,9
Net Sensible Cooling Capacity kW	31,9
nSHR	1
Unit Net Sensible EER	3,36
Airflow m3 /h	8163
Compressor modulation 40% (*)	
Net Total Cooling Capacity kW	18,2
Net Sensible Cooling Capacity kW	18,2
nSHR	1
Unit Net Sensible EER	4,76
Airflow m3 /h	4665

Units shall have a minimum 7" Touch Screen Display

A fully redundant cooling system is required. To achieve these two AC units are needed. The supplier should supply three AC systems, which will be working in tandem. Two AC systems should be up and running 24/7 and the third AC system should be on stand-by. In the case that the first AC system fails to provide the needed operation the third AC should act as the prime system. The supplier should

design and install the cooling system in such a way that the switch between two AC units can be done automatically and manually.

Cooling units shall be EUROVENT Certified.

9.6. Fire Detection and Suppression (Quantity 1)

The fire detection and suppression systems should consist of:

- Agent Tank/s (high strength steel cylinders)
- Agent
- Distribution Piping Network
- Nozzles
- Smoke/fire sensors
- Detection control panel
- **System should be able to send email and SMS notification**

Fire Detection System - environmental monitoring system with all components (Smoke detect sensors and alarms) shall include

- Interactive Addressable Fire Alarm panel - one signal loop 125 addresses and
- Combined optical smoke and heat detectors
- Addressable Manual call point with BREAKABLE glass
- Addressable Sounder with flash
- Outdoor siren

The Fire Extinguishing (suppression) System will be a Novec 1230 based solution shall be installed, consisting of:

- 3 zone EP extinguishant control panel (to BS/EN12094-1) c/w 3A EN54-4 PSU & 128 x64 pixel graphical
 - Plastic box single for emergency stop with modul for hold and abort
 - ActiV combined optical + heat Multi -Sensor detectors
 - Indoor siren – 90dB
 - Outdoor siren – metal box, with flash 110 dB
 - Discharge pressure switch wired for a discharge input to the system control panel
 - Nozzles with drilled hole calculated by a certified software
 - Gas Novec 1230 3M™ Novec™ 1230 filled in cylinder acc. Hydraulic calculation
- Gas Suppression System is a Data Center grade solution.

The system should involve safety features like “Lock Out/Abort Switch” and “Manual Pull Station”.

Lock Out/Abort Switch -This feature is essential for instances when a staff is in the protected environment and creates smoke. A lock out/abort switch should disable the system to avoid an accidental discharge. If a threatening fire starts while the system is disabled, the staff should arm the system using the manual pull station.

Manual Pull Station -If a fire is inadvertently started, or is noticed by someone in the room, the manual pull station allows for immediate system activation without waiting for the system to detect smoke.

The system should be capable of being operated under all circumstances, including power failure. Regular maintenance and cleaning are necessary for the fire detection system and corresponding accessories.

No matter the system is in manual or automatic mode, an elapsed time of at least 30 seconds is required for personnel evacuation before the gas is released. To facilitate evacuation, all emergency exits should be labeled with battery supported illumination.

9.7. Electrical System (Quantity 1)

Electrical installations shall be Tier 3, based on calculated IT and non-IT load.

All cables shall be properly dimensioned and fire resistant.

In order to achieve Tier 3, at least five electrical distribution cabinets shall be installed (MDB A, MDB B, UPS DB A, UPS DB B, L & SP DB)

MDB A and MDB B cabinets are main electrical cabinets

UPS DB A and UPS DB B are UPS distribution cabinets (including UPS bypass)

L & SP DB cabinet is for power distribution to devices not connected to UPS (lighting, utility sockets, etc.)

Cable trays shall be metallic, installed under the raised floor.

LED lighting inside the Data Center shall be installed.

Emergency lighting has to be installed also.

At least 6 utility sockets, not connected to UPS shall be installed.

9.8. UPS System (Quantity 1)

A highly efficient 3-phase scalable UPS should be installed. The UPS is expected to be located on the ground floor, vertically below the Primary Data Center on the third floor. All power linkages to the PDC, security considerations, environmental control and emergency systems should be considered as part of the total UPS requirements. The UPS should have an output power not less than 90KW and has the following requirements:

Modular UPS power cabinet

Modular battery cabinet

High power density 30kW power modules at ambient temperature 0-30 Degree

Three integrated hot swappable power models, space for additional 2

Ten integrated battery modules enabling 15 minutes of autonomy for 60 KW load, space for additional 5 modules.

High efficiency with load bigger than 30% the efficiency is more than 96% in normal operation (dual-conversion mode).

Splitted bypass can be connected.

Hot-swappable power modules.

Distributed intelligence (each power module is independently controlled by his own logic; it means in case of a broken module the other will still run).

Choice of Internal modular batteries or external traditional with wide range of DC bus voltage

Rack looking design of the body, easy to fit in data center application

In-rack tower should be included in the maintenance bypass switch for full power.

Ready for bottom and top cable entry.

Each battery module should have its own battery circuit breaker

IS-UNITY-DP - IntelliSlot Unity card with SNMP/Web, Modbus and BACnet communication card

All units (UPS, HVAC, Generator, PDU) will send SNMP traps to a central monitoring system. This system will be also polling to these devices. All alerts and alarms based on a predefined alarm severity and actions will be sent to a Data Center maintenance team. Central monitoring system, which will enable alarm analyses and definition of actions with few levels of acknowledgment and alarm history should be implemented.

System needs to be able to send 'SMS or email' or 'SMS and email' notification.

Relay Card with 18 contacts and possibility to shut down the UPS.

AC - AC online double conversion Between 95% and 96% for load >30%

Input Parameters

Rated input voltage 380/400/415 VAC, three-phase four-wire

Rated operating frequency 50/60Hz

Input voltage range 305V - 477V at full load, -25% to -40% with linear load de-rating

Input frequency range 40Hz - 60Hz

Input power factor >0.99

Input THDI <3%

Battery Compensation Yes

Charger output voltage regulation accuracy 1%

Output Parameter

Inverter output voltage 380/400/415 VAC, three-phase four-wire

Inverter output frequency 50/60Hz

Output frequency stability 50Hz/60Hz±0.02%

Bypass Parameter

Bypass input voltage 380/400/415 VAC, three-phase four-wire

Environmental Conditions

Operating temperature range 0 - 40°C*

Storage temperature -25 to 70°C

Relative Humidity ≤95%

Noise (1m) 52 - 62 dBA, adjusted according to load rate and number of modules

IP Class IP20

Standards

Low Voltage Directive 2006/95/EC with the Amendment Directive 93/68/EEC Directive for electromagnetic compatibility 2004/108/EC

General and safety requirements for UPS used in operator access areas IEC/EN 62040-1-1 incorporating requirements of IEC/EN 60950-1

Electromagnetic compatibility (EMC) requirements for UPS IEC/EN 62040-2: Immunity category C2, Emission category C2

Method of specifying the performance and test requirements of UPS IEC/EN/AS 62040-3

9.9. Diesel Power Generator (Quantity 2)

A three-phase diesel power generator with a heavy duty, 4-cycle, diesel engine should be provided to offer backup power to the facility. The diesel generator should meet the following requirements:

Backup Generators, 400/230 V - THREE-PHASE, 1.500 R.P.M., 50 Hz, LTP 135 KVA, RTP 125 KVA.

- Including ATS.
- Fuel tank at least 220l.
- Integrated SNMP monitoring card.
- Engine/alternator monobloc directly connected and installed via silent blocks on a frame made from high tensile electro welded steel profiles that are treated with degreasing liquids and applied with a phosphate coat and Polyester (QUALICOAT) paint.
- Canopy of steel sheet sound proofed with fireproof rockwool and treated with degreasing liquids and applied with a phosphate coat and Polyester (QUALICOAT) paint.
- Sealed chassis Fuel tank integrated in the chassis provided with fuel level gauge and fuel lines to the engine.
- Engine with mechanical engine driven pusher fan.
- Residential silencer with -35 dB(a) noise reduction with exhaust tube and protection cap.
- Thermal and magnetic circuit breaker
- Battery charge alternator.
- Starter battery complete with cables to the engine and pole protection.
- External emergency stop push button.
- Self-excited and auto regulated alternator.
- Base frame prepared for trailer kit Standard electronic speed governor on engines
- Electric control cubicle with digital control module, automatic mains failure, manual start, or remote start on signal.

- Battery charger for gen set with 12VCC battery (3A). Battery charger for gen set with 24VCC battery (5A).
- Electric engine coolant preheating.

The generator accepts 100% rated load in one-step and meets ISO 8528-5 class G-3 for transient response

Control Unit: Microprocessor based control panel, 12 or 24 Volt DC compatible.

Metering via LED display: Generator Volts, Engine oil pressure, Generator Ampere, Engine temperature, Generator Frequency, Plant battery volts, Engine hours run, Mains Volts

Alarms: Over and Under Speed, Low and High Battery Volt, Start and Stop Failure, Charge fail, Under / Over Generator Voltage, Low Oil Pressure, Emergency stop, High engine temperature

An Automatic Transfer Switch (ATS) should be supplied. ATS should provide a seamless transition between the primary source of power and the diesel generator.

UPS systems should send alarms for all events defined as critical. One of these alarms is also "Power on Battery" which indicates that there is no power from the grid. The system should be able to send 'SMS or email' or 'SMS and email' notification

ATS should come combined with a control panel (CP). Once the ATS detects a loss of power from the primary source it should send a signal to the generator to start and resume power to the facility. As soon as the primary source power has resumed, the Automatic Transfer Switch automatically transfers power needs back to the primary source and shuts the generator down. All this should be done without any human intervention. ATS should come with at least three operating modes: Automatic, Manual and Off. The ATS should be fully integrated with the diesel power generator.

A generator enclosure should also be provided by the contractor. A concrete slab must be installed of appropriate size, thickness, and construction (reinforced concrete) to accommodate the 2 generators and allow for adequate room for maintenance, servicing, fueling, etc. The generator enclosure should be securely fenced to ensure security and allow access only to authorised personnel.

The location of the generator enclosure shall be agreed upon consultation with the NCRA and included in all relevant design documents.

9.10. Installation, Testing and Documentation

The Vendor should supply all the equipment and/or services mentioned in this document. The supplier shall unpack the products, inspect for damage, install in accordance with original product vendor specifications, and run a complete operational test.

Proper labelling is crucial to the successful management of Server Room infrastructure. Labelling in the Server Room assists in determining locations of components and defining the system connections. Identification of Server Room shall conform to ANSI/TIA/EIA-606(A) standards.

The Supplier shall supply the following set of documentation:

- Product literature, describing the different systems/equipment components.
- Full map of the implemented architecture, detailed schema for each system and installations (network, electrical, HVAC, Security Systems etc.).
- Support, operations, and maintenance documentation through hard and soft copies on CD/DVD-ROM.
- End-user documentation.

All user documentation shall be provided in English.

At the end of the installation, the following documentation shall be provided:

- Original test data.
- Warranty Certificate.
- Server Room Cabling Infrastructure Layout.
- Labelling schemes.

Electrical safety and bonding tests shall be carried out according to IEC standards.

Other requirements

Certificate

The offered products should bear a CE marking symbolizing conformity with all available Community provisions and directives.

9.11. Warranties

The Contractor shall provide all equipment with a minimum three (3) year warranty and support.

10. Specifications and Requirements of the Primary Data Center.

10.1. Server Racks and PDU (Quantity 6)

Server Rack enclosures are designed for secure, high-density server and networking applications in IT environments. Designed with provisions to integrate power distribution and cable management, Server Rack enclosures make ideal homes for mission-critical equipment. In order to provide additional work after the server room is functional, all the supported Racks should be installed from the beginning. This means that the supplier should provide 42U Racks, fix them in the raised floor and install all the other components like power and data cables.

Racks shall be:

- 42U racks network and server rack, made of stable, lightweight aluminum profiles, connected with die cast corner joints, rack completely assembled, demountable on site, completely grounded (EN 60950), load rating 8000 N,
- Height 2000 mm, Width 600 mm, Depth 1200 mm
- Single Sheet Steel Front-Door 83% Perforation,
- Double Sheet Steel Rear-Door 83% Perforation,
- 19" Server Vertical Extrusion, U Markings, Front,
- 19" Server Vertical Extrusion, U Markings, Rear,
- Top Cover, With Cut Out for Fan Units, Cable Inlet Rear,
- Adjustable Feet (0-25 mm),
- Side Panel Both Sides,

On each rack, 2 (two) PDU units shall be installed (Side A and Side B)

PDU shall be:

- Monitored, 0U, input IEC 60309 230/400V 3x16A, (36)C13 (6)C19
- 2 PDU units for each rack
- Rating: 16A 3~ WYE 230/415V max, 24A 3~ Delta 208V max, 48A 1~ 240V max
- Sockets: (30) U-Lock C13, (6) U-Lock C19
- Network Connection: Dual 10/100Mbps Ethernet
- Protocols supported: DHCP, HTTP, HTTPS, IPv4, IPv6, LDAP, NTP, RSTP, SSH, SMTP, SNMP (v1/v2c/v3), Syslog

Remote sensor RJ connection jacks: 1 (Support for up to 16 Sensors).

10.2. Blade Enclosure (Quantity 2)

- Solution should house the required number of blade servers in fully redundant and high available enclosures. Should support a minimum of 8 half height blades in the same enclosure, occupying a max of 6U rack height.
- Should be able to accommodate the blade servers mentioned in the specifications, in the proposed enclosure in mixed configuration with half height and full height Blades within the same chassis.
- Minimum 2x Network module / switch must be included with the following features:
 - 10Gbps based CEE converged LAN / SAN network (Virtual / Converged Fabric)
 - FCoE backing 802.1Qbb, DCBX, IEEE 802.1Qaz
 - Minimum 8x 10Gbps Ethernet SFP+ uplink port with all the licenses
 - Internal connections to servers at least 30Gb per server
 - Must support SFP and direct-attach-cables
 - Must be fully controllable via management system with all involved licenses
 - Converged fabric - supports Ethernet and FCoE with all the licenses
 - Management
 - Ether Channel, LACP
 - QoS coherent with other network elements (matching, marking, policing)
 - IEEE 802.1Q VLAN encapsulation
 - IEEE 802.3x Full-Duplex Flow Control
 - IEEE 802.1p Tagged Packets
 - Redundancy - Layer 2 Trunk Failover to support active / standby
 - 8 x 10GBASE-SR SFP+ Module per chassis
- The enclosure should be fully populated with power supplies of the highest capacity available from the vendor.
- Fully populated with Hot Swap & Redundant variable Speed blowers/Fan Modules. 3years' warranty and support.
- MAF (Manufacturer Authorization Form) – mandatory.

Installation, testing and startup: Contractor shall unpack the product, inspect for damage, install in accordance with original product vendor specifications, run standard test and diagnostics routines, and install appropriate service tools; physically connect the equipment to a network, LAN, or WAN as appropriate, perform system power up and self-test, verify equipment operations and ensure that the current software and firmware is loaded on the product. Product has to be inserted into the rack. All management, performance and network tools configured and operational by default configurations.

10.3. Blade Servers (Quantity 16)

- Server solution must be from the same vendor with the technical requirements of Blade shelf (enclosure)
 - Latest generation of 2 x CPU Intel Xeon Processors (or equivalent) with 16 cores (min 22M Cache or higher, 2.0 GHz or higher),
 - 256 GB DDR-4 LRDIMM Memory (scalable to 1TB) with memory protection features, 19200MHz or higher.
 - Integrated Hardware Disk Controller to support RAID 1
 - The server should support SAS, SATA, and SSD hard disk drives
 - Should include at least SAS 2 hard drives with minimum capacity of 480 GB 12G SSD HDD
 - Should have at least 2 40Gbps Ethernet ports that are FCoE-capable
 - Support at least 40Gbps m-LOM for blade servers
 - OS and Virtualization Software Support for VMware, Microsoft Windows, Server, RHEL, SLES, Oracle Solaris.
 - Hypervisor software licenses included for all server processors, including VMware ESXi and vCenter.
- 3 years warranty and support.
- MAF (Manufacturer Authorization Form) – mandatory.

Installation, testing and startup: Contractor shall unpack the product, inspect for damage, install in accordance with original product vendor specifications, run standard test and diagnostics routines, and install appropriate service tools; physically connect the equipment to a network, LAN, or WAN as appropriate, perform system power up and self-test, verify equipment operations and ensure that the current software and firmware is loaded on the product. Product has to be inserted into the rack. All

management, performance and network tools configured and operational by default configurations.
Integration in existing IT system

The contractor should provide all the necessary components for the solution to be workable.

10.4. Fabric Interconnects (Quantity 2)

- Solution should include two appliance devices working in the cluster. Providing the network connectivity for the servers and their management. The proposed computing platform must have a single integrated management application for all aspects of configuration, management, monitoring, alerting and security.
- The devices should have at least:
 - 24 ports that support:
 - 40 Gbit/s Ethernet
 - 40 Gbit/s FCoE
 - 16 ports that support:
 - 1/10 Gbit/s Ethernet
 - 8/16Gbit/s FC
 - 8 x 10GBASE-SR SFP Module per switch
 - 8 x 16 Gbps Fibre Channel SW SFP+, LC, per switch
 - Minimum 16 ports licensed for 10GE/FC ports per switch
- Devices should have line-rate performance.
- Devices should have at least 8 hardware queues per port
- Devices should support at least 2000 VLANs
- Throughput of the devices must be min 2.4 Tbps.
- Standards and features supported
 - IEEE 802.1p: CoS prioritization
 - IEEE 802.1Q: VLAN tagging
 - IEEE 802.1s: Multiple VLAN instances of Spanning Tree Protocol
 - IEEE 802.1w: Rapid reconfiguration of Spanning Tree Protocol
 - IEEE 802.3: Ethernet
 - IEEE 802.3ad: LACP
 - IEEE 802.3ae: 10 Gigabit Ethernet
 - IEEE 802.3bg: 40 Gigabit Ethernet
 - SFP+ support
 - Remote Monitor (RMON)
 - Scalability to 20 blade chassis without adding complexity by eliminating the need for dedicated chassis management and blade switches and by reducing the number of cables needed
- 3 years warranty and support.
- MAF (Manufacturer Authorization Form) – mandatory.
- **Installation, testing and startup:** Contractor shall unpack the product, inspect for damage, install in accordance with original product vendor specifications, run standard test and diagnostics routines, and install appropriate service tools; physically connect the equipment to a network, LAN, or WAN as appropriate, perform system power up and self-test, verify equipment operations and ensure that the current software and firmware is loaded on the product. Product has to be inserted into the rack. All management, performance and network tools configured and operational by default configurations. Integration with the existing IT system.
- **Certificate:** The offered product should bear a CE marking symbolizing conformity with all available Community provisions and directives
- **The contractor should provide all the necessary components for the solution to be workable.**

10.5. Storage Systems (Quantity 2)

- Midrange hybrid storage system to provide redundancy, scalability, and high availability, with no single point of failure. Should have at least two redundant storage controllers working in an active/active mode. Connection between controllers should be via backplane or via direct connected cables.
- The storage controllers should have at least 2 x single-socket Intel Xeon™ (or equivalent) 1.7GHz CPUs, supporting at least 12 cores per storage array.
- Minimum 128GB cache memory per system (64GB per controller).
- The system should provide support for additional flash read/write cache memory, which should be expandable to up to minimum 800GB usable memory with SSD/Flash Drives within the storage system.
- Support for 12Gb/s drives (SSD Flash and HDD drives). At least 4 x 12Gb/s SAS ports for backend drive connection.
- Must support the minimum following protocols: FC, iSCSI, CIFS (SMB 1), SMB 2 and SMB 3, NFSv4 and above, FTP, SFTP and Vvols 2.0. Licenses for all protocols should be included. Extension to Unified storage with NAS support should be done through adding only additional ethernet ports (no NAS gateways, controllers, etc.) with a support of max file system size of 256TB.
- Expandable to a minimum of 500 drives.
- Must support 2.4PBs of internal raw storage capacity.
- Must have functionality of de-stage to disk safely by lowering the data from the memory cache.
- Should support 16Gb FC host ports and 10Gb/25Gb iSCSI/NFS/SMB ports.
- Min 4 x 16Gb FC host ports.
- Capacity: The proposed storage should be configured with at least: 50TB raw storage.
- Storage should also support SSD and HDD disks with different capacities. Spare drives for each drive type should be additionally included as per vendor best practices.
- The whole mentioned capacity will be 100% virtually provisioned which means that full license should be included for the whole capacity.
- Minimum RAID Levels supported: RAID 1/0, 5, 6
- Support for inline compression and deduplication (All-flash pools, Block and File).
- Support for controller-based Data-at-Rest encryption, with self-managed keys or external key management, to be able to encrypt data on physical drives.
- Ability for online migration of storage volumes of different drive types and RAID protections.
- The following tools should be supported and with included licenses for the whole capacity:
 - CLI and HTML 5.0 GUI web-based management
 - Real time and historical performance analysis, reporting and capacity management
 - Cloud-based storage analytics, allowing for proactive monitoring and predictive analytics support
 - Local point-in-time copies (snapshots and thin clones)
 - Data compression and deduplication on block and file level
 - QoS tools, with possibility to limit the IOPS/bandwidth per LUN/group of LUNs.
 - Virtual/Thin provisioning
 - IP Multi-tenancy
 - File-level retention (FLR-E and FLR-C)
 - Adapter for integration with VMware vSphere
 - Support for VAAI, VASA, VVOL and ODX
 - Support to change RAID level of volume online
 - Proactive support with Dial-home functionality
- Software for synchronous and asynchronous (Block and File) remote replication must be offered for the total capacity.
- Support for point in time copies (snap and/or thin clone), including a software tool for creation of application consistent point in time copies for different applications such as MS Exchange, Oracle, and MS SQL. License for at least 20 simultaneous crash-consistent application copies need to be included.
- Support for automatic and non-disruptive tiering of data to private and public cloud environments.
- Supported operating systems: Microsoft Windows Server, Linux, Oracle Solaris, VMware ESXi, IBM AIX, HP-UX
- 3 years warranty and 3 years support/maintenance.
- MAF (Manufacturer Authorization Form) – Mandatory
- **Installation, testing and startup:** Contractor shall unpack the product, inspect for damage, install in accordance with original product vendor specifications, run standard test and diagnostics routines, and install appropriate service tools; physically connect the equipment to a network, LAN, or WAN

as appropriate, perform system power up and self-test, verify equipment operations and ensure that the current software and firmware is loaded on the product. Product has to be inserted into the rack. All management, performance and network tools configured and operational by default configurations. Integration in the existing IT system.

- **Certificate:** The offered product should bear a CE marking symbolizing conformity with all available Community provisions and directives

The contractor should provide all the necessary components for the solution to be workable.

10.6. Tape Library (Quantity 1)

- Minimum LTO-8 Tape Drive FC Technology Host
- Connection:
- Minimum 2 FC Ports
- Slots:
- Minimum 40 Slots within Tape Autoloader
- Form Factor:
- 3U per module to a maximum of 21U
- Power Supply:
- Redundant Power Supplies
- Tape Cartridges:
- Minimum 1 Tape Cartridge LTO8 for each slot.
 - Minimum 1 Cleaning Tape per Autoloader,
 - Included 20 Tape Cartridges.
- Warranty
- Minimum 3 Years Warranty and Support

The contractor should provide all the necessary components for the solution to be workable.

10.7. Routers (Quantity 2)

- Each service-module slot should offer high data-throughput capability up to 10Gbps toward the router processor and to other module slots.
- Should support for both single and double wide service modules providing flexibility in deployment options.
- Should be able to increase the interface density with a carrier card that supports network interface modules in a service-module slot.
- Service modules should support online insertion and removal by reducing downtime required for new or replacement modules.
- Should have minimum 3 x Integrated NIM slots in order to allow for flexible configurations.
- Each NIM slot should offer high-data-throughput capability up to 2Gbps toward the router processor and to other module slots.
- Should have minimum 1 x single flash memory slot in order to support high-speed storage densities upgradable to 32GB
- Should support minimum 2 x USB type A 2.0 ports by providing secure token capabilities and convenient storage
- Should support 4-GB RAM memory.
- Should have Dual integrated power supplies provide power redundancy and industry-leading power efficiency.
- Should support the protocols such as IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IP sec, etc.
- Min support for IPSec tunnels with IKE/IKEv2 session control and following protection methods: Encryption: DES, 3DES, AES-128 и AES-256.

- Authentication: RSA (748/1024/2048bit), ECDSA (256/384 bit); Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512; More than 225 IPSec tunnels Generic routing encapsulation (GRE)

Should have minimum:

- 4 x WAN or LAN 10/100/1000 integrated RJ-45 or SFP based ports
- 2x 10Gig SFP+ WAN interfaces.
- additional 2 GE WAN NIM, dual-mode RJ45 & SFP
- Serial auxiliary port - RJ45
- Flash memory 8Gb upgradable up to 32GB
- Aggregate Throughput min 2Gbps
- Redundant AC power supply 100 to 240VAC auto ranging. Min 2 x 450W AC Power Supply

Min following security features must be included:

- Stateful inspection firewall
- Filtering based on Layer 3 and Layer 4 information
- Zone based firewall

Min the following virtualization features need to be included:

- Routing tables, protocols, and IP interfaces
- IPSec tunnels
- Integrated Firewall
- DHCP server services
- NAT

- Min the following routing protocols need to be included:

- Static routing for Ipv4 and Ipv6
- RIPv1, RIPv2
- OSPFv2
- BGP4 and BGP4+
- System-to-Intermediate System (IS-IS)
- Multicast Internet Group Management Protocol Version 3 (IGMPv3)
- Multicast routing with PIM SM и PIM SSM
- Policy based routing (PBR)
- Dynamic traffic routing through IPSec tunnels based on packet lost, jitter and delay parameters, automatically measured.
- VRRP
- Warranty: min. 3 Years Warranty and Support
- MAF (Manufacturer Authorization Form) – mandatory.

The contractor should provide all the necessary components for the solution to be workable.

10.8. Firewalls (Quantity 2)

- Next Generation Firewall System with dedicated Management
- Modular 1RU device, with at least 8 x 1/10 Gig ports for user traffic
- At least 1 Gigabit Ethernet port for out of band management
- The system must have Stateful Inspection firewall throughput with application control 12 Gbps
- The system must have max. firewall throughput with application control and NGIPS 10 Gbps
- The system must have support for at least 1000 VLAN interfaces
- The system must have redundant AC supply and 200 GB storage
- Support for static, BGP, and OSPF routing protocols
- Support for L2 transparent or routed mode and combination of them
- Possibility to allocate interfaces to work in IPS inline, inline TAP and passive mode
- The system must have IP, URL and DNS Reputation services provided by the vendor.
- The system must have Active-Standby HA.
- The system must support clustering of at least 6 units to increase throughput, concurrent connections, and new sessions/sec performance
- The Application Control and IPS system must have detection rules based on an open-source language to allow users to create their own rules, as well as to customize any vendor- provided rules
- Application control system

- Support for file reputation analysis, suspicious file sandboxing and retrospective reporting for files changing reputation over time
- The intrusion detection engine must be capable of inspecting traffic associated with different network segments differently.

The proposed Firewall systems must use dedicated external Management Servers for policy management, event, and information management– within a single web-based interface:

- The solution must be deployed as dedicated dual appliances each with 2 x 1 Gbps and 900GB event storage
- The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities
- The system must be able to automatically adapt defenses to dynamic changes in the network, in files or with hosts, without the need for administrator intervention.
- The solution must be capable of gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.
- The system must have Impact flags to automatically alert to the most critical events
- The system must have actionable indications of compromise to correlate network event information
- The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication
- The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.
- The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to hardware.
- The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered.
- The communications between the management platform and the Firewall must be secure.
- System should be shipped with all necessary vendor hardware and software services to replace the defective hardware and access to the manufacturer's technical center as well as the licenses for the detection and control of applications, malware file analysis and blocking, and IPS inspection for a minimum period of 3 years.
- License for threat defense, malware protection and URL Filtering included.
- Warranty: min. 3 Years Warranty and Support
- MAF (Manufacturer Authorization Form) – mandatory.

The contractor should provide all the necessary components for the solution to be workable.

10.9. Core Network Distribution Switches (Quantity 2)

Rack-unit (1RU) switch

The uplink can support up to six 40 Gbps ports, or a combination of 10-, 25-, 40-, 50-, and 100-Gbps connectivity, offering flexible migration options.

- Ports: 48 x 10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports
 - Max QSFP Transceivers included
 - At least 2x 10Gbps Transceivers included
- Management ports: 1 RJ-45 port
- USB ports:1

- Serial ports:1
- Frequency (AC): 50 to 60 Hz
- Fans:4
- Airflow: Port-side intake and exhaust
- RoHS compliance: Yes
- CPU: 4 cores
- System memory: 24GB
- SSD drive: 64GB
- System buffer:40 MB
- Management ports: 2 ports: 1xRJ-45 and 1xSFP
- Dual Power supplies: 650W AC
- Input voltage (AC): 100 to 240V
- MTBF at least 237,500 hours
- Warranty: min. 3 Years Warranty and Support
- MAF (Manufacturer Authorization Form) – mandatory.

The contractor should provide all the necessary components for the solution to be workable.

10.10. Edge Network and Management Switches (Quantity 3)

The minimum requirements:

- The switch must be designed to fit into a 19 "rack and must be at most 1RU high
 - Cooling airflow must be from front to back
 - The switch must be designed for trouble-free operation at ambient temperatures of -5°C to +45 °C and air humidity of 5% to 90%.
 - Switch must have a declared mean time between MTBF failures of at least 500000 hours
 - Switch must support the installation of a 220 VAC redundant power module
 - Switch must have at least two field replicable fan modules installed
 - Switch must have 24 integrated 10/100/1000Base-T Downlink ports with RJ-45 connector
 - Switch must have a 4x10 Gig SFP+ uplink interfaces.
 - Switches must support stacking of up to 8 switches in a single stack via optional stacking module. Switches in stack must support Stacking bandwidth of at least 80 Gbps. The stacking module and the cables does not have to be shipped with the switch.
 - Switch must have a Secure boot mechanism in place and mechanisms that ensure and validate the authenticity and integrity of the switch genuine hardware and software.
 - Switch must support a Control Plane Policing mechanism
 - Software (operating system) running on the switch must be digitally signed.
 - Switch must have a built-in RFID tag that makes it easy to manage assets / inventory with commercial RFID readers
 - The switch must have a built-in LED indicator for easy identification
 - Switch must support IEEE 802.1D, 802.1S, 802.1W, 802.3ad LACP, PAgP, LLDP
 - Switch must support IPv4 static routing, Inter-VLAN routing, RIP and OSPF routing protocols
 - Switch must support IPv6 static routing and RIPng
 - Switch must support Policy based routing - PBR routing
 - Switch must support VRRP protocol
 - Switch must support Flexible Netflow or IPFIX protocol for exporting traffic flow information
 - Switch must support SNMP, HTTP, HTTPS, SSH, Telnet management and monitoring protocols
 - Switch must support NETCONF, RESTCONF, gRPC protocols and YANG modeling
 - Switch must support L2 encryption according to IEEE802.1AE (MACSec) using AES-128
 - Switch must support IEEE 802.1x protocol
- Switch must have following characteristics and performance:
- Switching capacity of at least 128 Gbps
 - Forwarding performance minimum 95 Mpps
 - Switches must support at least 16000 MAC addresses
 - Support for at least 3000 IPv4 routes
 - Switches must support at least 1000 multicast routes
 - Switches must support at least 1000 QoS entries

- Support for at least 1,500 access control entry entries
- Buffer of at least 6MB
- Switches must support at least 16000 Netflow / sflow streams
- At least 2GB of DRAM memory
- At least 4GB of flash memory
- Switches must support 9198 bytes jumbo frames
- The switch must support 4096 VLAN ID
- Switches must support at least 500 logical L3 interfaces (SVI)
- Warranty: min. 3 Years Warranty and Support
- MAF (Manufacturer Authorization Form) – mandatory.

The contractor should provide all the necessary components for the solution to be workable.

10.11. Access Switches (Quantity 2)

The minimum requirements:

- L2 / L3 network switch with the following features:
- The switch must be designed to fit into a 19 "rack and must be at most 1RU high
- Cooling airflow must be from front to back
- The switch must be designed for trouble-free operation at ambient temperatures of -5°C to +45 °C and air humidity of 5% to 90%.
- Switch must have a declared mean time between MTBF failures of at least 340000 hours
- Switch must support the installation of a 230 VAC redundant power module
- Switch must have at least two field replicable fan modules installed
- Switch must have 48 integrated 10/100/1000Base-T Downlink PoE+ ports with RJ-45 connector.
- Switch must have a 4x1 Gig SFP+ uplink interfaces.
- Switches must support stacking of up to 8 switches in a single stack via optional stacking module. Switches in stack must support
- Stacking bandwidth of at least 80 Gbps. The stacking module and the cables does not have to be shipped with the switch.
- Switch must have a Secure boot mechanism in place and mechanisms that ensure and validate the authenticity and integrity of the switch genuine hardware and software.
- Switch must support a Control Plane Policing mechanism
- Software (operating system) running on the switch must be digitally signed.
- Switch must have a built-in RFID tag that makes it easy to manage assets / inventory with commercial RFID readers
- The switch must have a built-in LED indicator for easy identification
- Switch must support IEEE 802.1D, 802.1S, 802.1W, 802.3ad LACP, PAgP, LLDP
- Switch must support IPv4 static routing, Inter-VLAN routing, RIP and OSPF routing protocols
- Switch must support IPv6 static routing and RIPng
- Switch must support Policy based routing - PBR routing
- Switch must support VRRP protocol
- Switch must support Flexible Netflow or IPFIX protocol for exporting traffic flow information
- Switch must support SNMP, HTTP, HTTPS, SSH, Telnet management and monitoring protocols
- Switch must support NETCONF, RESTCONF, gRPC protocols and YANG modeling
- Switch must support L2 encryption according to IEEE802.1AE (MACSec) using AES-128
- Switch must support IEEE 802.1x protocol
- Switch must have following characteristics and performance:
- Switching capacity of at least 104 Gbps
- Forwarding performance minimum 77.38 Mpps
- Switches must support at least 16000 MAC addresses
- Support for at least 3000 IPv4 routes
- Switches must support at least 1000 multicast routes
- Switches must support at least 1000 QoS entries
- Support for at least 1,500 access control entry entries
- Buffer of at least 6MB
- Switches must support at least 16000 Netflow / sflow streams
- At least 2GB of DRAM memory
- At least 4GB of flash memory

- Switches must support 9198 bytes jumbo frames
- The switch must support 4096 VLAN ID
- Switches must support at least 1000 logical L3 interfaces (SVI)
- Warranty: min. 3 Years Warranty and Support
- MAF (Manufacturer Authorization Form) – mandatory.

The contractor should provide all the necessary components for the solution to be workable.

10.12. MDS Switches (Quantity 2)

- Supported Protocols:
 - Fibre Channel classes of service: Class 2, Class 3, и Class F
 - Fibre Channel standard port types: E, F and FL
 - Fibre Channel enhanced port types: SD, ST, and TE
 - FC-NVMe
 - In-band management using IP over Fibre Channel (RFC 2625)
 - IPv6, IPv4, and Address Resolution Protocol (ARP) over Fibre Channel (RFC 4338)
 - Extensive IETF-standards-based TCP/IP, SNMPv3, and remote monitoring (RMON) MIBs
- Ports:
 - Minimum 48 ports with the support for 4/8/16 Gbps FC
 - Minimum 12 port license included
 - Possibility to incrementally increase the base of a group of 12 ports, with 12-ports bundle license for activation
 - SFPs modules need to be provided based on the solution.
- Minimum the following security functionalities and protocols must be included:
 - Role-based access control (RBAC) using RADIUS, TACACS+, or LDAP AAA functionality.
 - Secure FTP (SFTP)
 - Secure Shell Protocol Version 2 (SSHv2)
 - Simple Network Management Protocol Version 3 (SNMPv3) with Advanced Encryption Standard (AES)
 - Control-plane security
- Performance:
 - Port Capacity: 2/4/8/16 Gbps auto sensing with 16 Gbps dedicated bandwidth per port.
 - 16Gbps, line rate, non-blocking, non-oversubscribed
 - PortChannel: up to 16 physical links.
- Management:
 - Ability for monitoring and alerting included
 - Out-of-band 10/100/1000 Ethernet port
 - RS-232 serial console port
 - USB
 - CLI using console and Ethernet ports
 - SNMPv3 using Ethernet port and in-band IP over Fiber Channel access
 - Per-VSAN RBAC using RADIUS and TACACS + based AAA functionalities
 - SFTP
 - SSHv2 implementing AES
 - SNMPv3 implementing AES
- Other features:
 - ISSU
 - Hot-swappable, dual redundant power supplies
 - Hot-swappable fan tray with integrated temperature and power management
 - Passive backplane
 - Stateful process restart
 - Online diagnostics
 - 100 to 240V AC (10% range)
 - 50 to 60 Hz (nominal)

- Airflow: back to front (toward ports)
- Programmable interface:
 - Scriptable CLI
 - Ability to use Network Management software with web services API
- Warranty: min. 3 Years Warranty and Support
- MAF (Manufacturer Authorization Form) – mandatory.

The contractor should provide all the necessary components for the solution to be workable.

10.13. Backup Software (Quantity 1)

- Backup & Replication - Maintenance 3 Years Upfront Billing & Production (24/7) Support
- Subscription license
- Virtual Machine: 30
- Physical server: 10
- Backup for VMs, servers and workstations (with advanced data reduction)
- Replication for VMs (environment replication for DR)
- Instant recovery on-premises and direct restore to the cloud
- Flexible granular recovery (file and application items)
- Deduplicating storage integrations
- Advanced tape support
- Backup I/O control
- Storage snapshot integration for the world's leading primary storage
- Comprehensive self-service capabilities for backup and restore
- Built-in WAN Acceleration (for backups, copies, and replicas)
- Enterprise Plug-ins for Oracle RMAN and SAP HANA
- NDMP to Tape (no per-TB charges)

10.14. KVM Switch (Quantity 1)

- Ports: 16 ports KVM Switch, with all cables and adapters for server connection included.
- Form: RACK Mountable 19" pull out screen with keyboard and pointing device.

10.15. Training (Quantity 1)

The Contractor should provide hands-on On-the-Job Training during implementation of the Server Room and Primary Data Center for NCRA staff that will be managing this infrastructure. Further details regarding the format, objectives, duration, expected participation numbers, any testing requirements, minimum pass marks, etc. are being requested from the client and shall be updated when available.

10.16. Warranties

The Contractor shall provide all equipment with a minimum three (3) year warranty and support.

10.17. Primary Data Center - Theoretical Schematic

