SOS Children's Villages Nepal

Request for Proposal

Network Infrastructure Upgrade Project 2026

1. Background

SOS Children's Villages Nepal is a not-for-profit social organisation that primarily works for the best interests of children who have lost parental care or are at risk of losing it. It contributes to provide basic rights in accordance with fundamental human rights principles and instruments such as the United Nations Guidelines on Alternative Care, the United Nations Convention on the Rights of the Child, and prevailing national law. The organisation operates a range of alternative care services, including family-like care, kinship care and small group homes. It also runs schools and training centres. Through its family strengthening programmes, it supports children and families by ensuring access to education, health, nutrition, hygiene and income-generating activities, which are fundamental to preventing family separation. SOS Children's Villages Nepal also actively advocates for the rights of children and young people across the country and provides emergency relief services when needed.

2. Project Objective

The objective of this project is to replace legacy network security appliances, and wireless access points that have reached or are approaching end-of-support, connecting two project locations using fiber, renewing existing network devices licenses, and switch installation using modern, next-generation solutions which are physically nearby. The upgraded infrastructure shall improve security, performance, resilience, and manageability while ensuring continuity of business operations.

3. Scope of Work

The scope of work shall include, but not be limited to, the following activities covering both network security appliances, network switch and wireless access points:

3.1 Assignment Locations

3.1.1 National Office (NO)

Work Required

- Configuration of the existing on-premises hardware server with a RADIUS service (Linux or Windows-based) and an internal Certificate Authority (CA) (both

installation and configuration), integrated with Microsoft Intune to enable certificate-based authentication.

- Renewal of Meraki switch license.
- Replacement of current firewalls with two firewalls in High Availability (HA) setup.
- Replacement of current wireless access points with new enterprise-grade access points.

Other Tasks:

- Supply, decommission, and physically install devices.
- Provision and stage devices with base configuration, firmware, and cloud/centralized registration.
- Migrate VLANs, VPNs, SSIDs, routing, and security policies.
- Configure RADIUS server, CA, and Intune certificate-based authentication for office Wi-Fi.
- Validate Wi-Fi coverage, authentication, and network performance.
- Perform fluke test of cat6 cable used for Access Points
- Perform testing, cutover, and rollback planning.

3.1.2 Child and Youth Care Practitioners' Training (CPT) Center, Kavre

Work Required:

- Install a new switch in place of the legacy Meraki network appliance.
- Connect using SFP and fiber that has already been pulled from SOS Children's Village Kavre to this location.
- Configure VLANs, routing, and security policies.
- Conduct Fluke testing of CAT6 cables used for Access Points and rectify any issues identified.
- Perform testing, cutover, and rollback planning.

3.1.3 SOS Children's Village (CV) Pokhara and Employment and entrepreneurship training (EET) Centre Pokhara

Work Required:

- Install a new switch in place of the legacy Meraki network appliance.
- Configure VLANs, routing, and security policies.
- Conduct Fluke testing of CAT6 cables used for Access Points and rectify any issues identified.
- Perform testing, cutover, and rollback planning.

3.1.4 Small Group Homes Sanothimi and Small Group Homes Jorpati

Work Required:

- Renewal of Meraki switch license.
- Connect two project locations: Small Group Homes Sanothimi → Small Group Homes Jorpati (~200 meters) both are located in Koteshwor.
- Pull fiber using SFPs to establish connectivity.
- Install switches in place of legacy Meraki firewalls.
- Replicate VLANs, routing, and security policies.
- Perform fluke test of cat6 cable used for Access Points.
- Perform testing, cutover, and rollback planning.

3.1.5 Rest of the Project Locations

Work Required:

- Renewal of Meraki switch license.
- Replace existing Meraki security appliances with new network security appliances.
- Replace existing Meraki wireless access points with enterprise-grade access points.
- Configure certificate-based authentication for office Wi-Fi.
- Perform Fluke Test of cat6 cable used for Access Points.
- Apply VLANs, routing, and security policies consistent with National Office deployment.

Other Scope of Work

3.2 Device Identification

- Annex B contains the information of items that needs to be procured, replaced and updated.
- The placement of devices such as network appliance, network switch and wireless access points shall remain the same as the current deployment.

3.3 Device Replacement

- Decommission legacy devices in a controlled manner.
- Perform physical installation (rack mounting for firewalls, switches, ceiling/wall for APs).
- Ensure proper power, cabling, and interface connectivity.

3.4 Provisioning & Staging

- Stage devices prior to deployment.
- Apply base system configuration and required firmware/software versions.
- Register devices to cloud-based management platforms.

- Maintain asset records including serial numbers, MAC addresses, and site assignments.

3.5 Migration and Cutover

- Migrate existing network and wireless configurations including VLANs, VPNs, SSIDs, routing, and security policies.
- Validate office Wi-Fi SSIDs using deployed certificates.
- Configure authentication and related settings on all wireless access points.
- Validate configuration consistency, optimization, and network performance.
- Execute production cutover with rollback planning.
- Minimize downtime and service impact during migration.

3.6 Documentation and Handover

- Provide as-built configuration documentation.
- Update physical and logical network diagrams.
- Deliver asset and license documentation.
- Conduct knowledge transfer and handover sessions for ICT staff.
- Ensure proper handover of all legacy devices to the relevant program/location in-charge.

3.7 Post-Implementation Support

- Provide post-deployment stabilization support for an agreed period.
- Resolve configuration or operational issues identified after go-live.
- Support fine-tuning and optimization if required.

4. Deliverables

- Deployed and commissioned network security appliances.
- Deployed and commissioned network switches.
- Deployed and commissioned enterprise wireless access points.
- Migration and testing completion report.
- Configuration and network documentation.
- Knowledge transfer completion sign-off.

5. Acceptance Criteria

- All legacy devices successfully replaced.
- Network services operating as expected.
- Wireless coverage and performance validated.
- Security policies enforced as per requirements.
- Formal acceptance by the organization.

6. Technical and Financial Requirements

6.1 Device Technical Requirements Sheet

All vendors are requested to submit detailed technical responses in a **separate sheet** as mentioned in Annex A along with the timeline and plan for the implementation. This sheet will include a checklist of all requirements for network security appliances, switches, fiber equipment, wireless access points and licences covering:

1. Network Security Appliance Requirements
2. Wireless Access Point Requirements
3. Network Switch Requirements
4. License Requirements

Note: Only submissions with the completed technical requirements sheet will be considered for evaluation.

6.2 Techical evaluation criteria of the bidders

The bidder shall be evaluated based on the following technical criteria:

- Company profile and relevant experience in similar network projects
- Compliance with technical specifications (Annex A, B, C) for firewalls, switches, wireless access points, fiber, and licenses
- Implementation methodology and deployment plan, including staging, cutover, and rollback strategy
- Project timeline and delivery capability
- Team qualifications and relevant certifications
- Past performance and client references
- Post-implementation support plan, including SLA, response time, and local support capability
- Quality of documentation and knowledge transfer approachs

6.3 Financial Proposal Requirements

The financial proposal should include all associated costs, including:

- Installation and setup cost as per the Scope of work in section 3.
- Device, equipment and license costs as specified in Annex B, aligned with the technical recommendations in Annex C
- Travel expenses for implementation, including food and accommodation for the entire deployment period
- Ensure that all costs are clearly itemized and aligned with the respective annexes.

7. **Sealed Proposal Submission Deadline**

The Service Provider shall submit sealed proposal along with legal documents (company registration and tax clearance certificate of fiscal year 2081/82) **on or before 5:00 pm of 30 April 2026**. Sealed proposals shall be clearly marked the subject with "Sealed Proposal for Network Infrastructure Upgrade" outside the envelope and submitted to the address mentioned below.

SOS Children's Villages Nepal

National Office

Sanothimi, Bhaktapur, Nepal

procurement@sosnepal.org.np

Annex A

Network Security Appliance Required Specifications for the National Office

Technical Specification of NO Firewall

S.N.	General	Technical Specification	Compliant (Yes/No)
A	Brand	To be Mentioned by bidder	
B	Model	To be Mentioned by Bidder	
C	Quantity	Refer Annex B	
D	Type	Type: Next Generation Enterprise Firewall should be deployed in HA	
1	Market Validation	The proposed solution should be in the LEADERS quadrant in the latest " Gartner Magic Quadrant for Hybrid Mesh Firewall" report.	
2	Interface	Firewall appliance should be supplied with at least 8 x 1GE RJ45 ports, 2x1G SFP, 1xMgmt Port and Console from day 1.	
3	Device Performance Capacity	The Firewall Threat Prevention (appmix/Ent.Mix/web Mix) throughput should be Minimum of 2 Gbps with IPS, antivirus, DNS Security, file blocking, and logging features enabled. Throughput under Testing Condition won't be considered.	
4		The Proposed Model must support atleast45k new sessions per second using 1 byte HTTP transactions or minimum 150K New Sessions per Seconds with TCP.	
5		Firewall should support at least 200k concurrent HTTP sessions or at least 900k concurrent TCP sessions.	
6		The proposed system should have 2Gbps VPN throughput.	
7		The proposed Firewall must provide 2000 IPSEC(G/W to G/W) VPN tunnel and 1000 SSL VPN users from day 1.	
8	Storage and RAM	Firewall must have at least 8 GB RAM and 120 GB Storage for Logging.	
9	Threat Prevention	Threat prevention signatures should be built based on the vulnerability itself. A single signature should stop	

		multiple exploit attempts on a known system or application vulnerability.	
10		The solution should be capable to provide deep learning and heuristic analysis engines to prevent known and unknown exploits, malware, spyware, malicious zero-day command-and-control (C2) attacks.	
11	**High Availability**	The proposed solution should support HA	
12		High Availability Configurations should support Active/Active and Active/ Passive	
13	**IT/IOT Security**	The solutions must provide visibility into IoT devices and identify the software libraries used on unmanaged devices and any associated vulnerabilities.	
14		Should Generate risk scores, based on the Common Vulnerability Scoring System (CVSS), provide an effective way to prioritize results, quickly exposing any behavioural anomalies and threat details for security teams to initiate a response and consistently reducing the attack surface area.	
15	**SDWAN**	The solutions must provide visibility into SD-WAN activity, enabling identifications of applications or links with performance issues. License of shared features should be bundled from day one.	
16		Must support real-time and historical views of path quality and link performance over a configurable time range.	
17	**DNS Security**	Should support prevention against advance DNS based attacks trying to abuse DNS Protocols.	
18		proposed solution should support DGA Based attacks, DNS Tunnelling attacks.	
19		DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command & Control.	
20	**License and Support**	The proposed solution should be quoted with 3 years OEM support and subscription for Firewall, Threat Prevention, Malware Protection, Application Control, Web-Filtering and DNS Security and OEM 24x7 TAC	

		Support along with license for all of the above mentioned features.	
21	**Central Manager**	The proposed solution should provide central console to managed proposed firewall from Cloud in Day one.	
		Should Provide best-practice recommendations and proven workflows to strengthen the organization's security posture and eliminate risk.	
		Should Provide a common alerting framework to identify network disruptions, enabling the organization to maintain optimal system health and performance.	
22	**Manufacturer Authorisation**	The manufacturer authorization letter should be provided specifically in the name of the bidder, authorizing them to supply, install, and support the offered solution directly from OEM to Customers Email	
23	**Local Experience**	The bidder must have past experience of deployment of similar solution in at least 3 Enterprise, Education, Health or government organization in Nepal. Proof of reference documents must be submitted.	
24	**Bidder Response**	The bidder is responsible for installation, performance tuning, onsite support during installation phase and configuration to ensure the firewall operates as proposed in the network environment. Should migrate existing firewall policy into new firewall along with the existing network with proper documentation.	

Fiber Equipment Required Specifications for the SOS Care Practitioner Training (CPT), Kavre, SOS SGH Jorpati & SOS EET, Pokhara

S. N	Device	Requirement Description	Proposed Brand and Model
1	Fiber	24 Core Fiber	
2	SFP	Modules (10G, SM, LC, 20km)	
3	Conduit	HDPE Conduit (25 mm)	

Network Security Appliance Required Specifications for branch locations

Technical Specification of Branch Firewall

S.N.	General	Technical Specification	Compliant (Yes/No)
A	**Brand**	*To be Mentioned by bidder*	
B	**Model**	*To be Mentioned by Bidder*	
C	**Quantity**	Refer Annex B	
D	**Type**	Type: Next Generation Enterprise Firewall	
1	**Market Validation**	The proposed solution should be in the LEADERS quadrant in the latest " Gartner Magic Quadrant for Hybrid Mesh Firewall" report.	
2	**Interface**	Firewall appliance should be supplied with at least 7 x 1GE RJ45 ports, 1xMgmt Port and Console from day 1.	
3	**Device Performance Capacity**	The Firewall Threat Prevention (appmix/Ent.Mix/web Mix) throughput should be Minimum of 800Mbps with IPS, antivirus, file blocking, and logging features enabled. Throughput under Testing Condition won't be considered.	
4		The Proposed Model must support at least 10k new sessions per second using 1 byte HTTP transactions or minimum 90K New Sessions per Seconds with TCP.	
5		Firewall should support at least 60k concurrent HTTP sessions or at least 300k concurrent TCP sessions.	
6		The proposed system should have 400mbps VPN throughput.	
7		The proposed Firewall must provide 500 IPSEC(G/W to G/W) VPN tunnel and 250 SSL VPN users from day 1.	

8	**Storage and RAM**	Firewall must have at least 8 GB RAM and 120 GB Storage for Logging.	
9	**Threat Prevention**	Threat prevention signatures should be built based on the vulnerability itself. A single signature should stop multiple exploit attempts on a known system or application vulnerability.	
10		The solution should be capable to provide deep learning and heuristic analysis engines to prevent known and unknown exploits, malware, spyware, malicious zero-day command-and-control (C2) attacks.	
11	**IT/IOT Security**	The solutions should support visibility into IoT devices and identify the software libraries used on unmanaged devices and any associated vulnerabilities.	
12		Should Generate risk scores, based on the Common Vulnerability Scoring System (CVSS), provide an effective way to prioritize results, quickly exposing any behavioural anomalies and threat details for security teams to initiate a response and consistently reducing the attack surface area.	
13	**SDWAN**	The solutions must provide visibility into SD-WAN activity, enabling identifications of applications or links with performance issues. License of shared features should be bundled from day one.	
14		Must support real-time and historical views of path quality and link performance over a configurable time range.	
17	**License and Support**	The proposed solution should be quoted with 3 years OEM support and subscription for Firewall, Threat Prevention, Application Control, SD-WAN, Web-Filtering and OEM 24x7 TAC Support.	
18	**Central Manager**	The proposed solution must provide central console to managed proposed firewall from Cloud in Day one.	
		Should Provide best-practice recommendations and proven workflows to strengthen the organization's security posture and eliminate risk.	
		Should Provide a common alerting framework to identify network disruptions, enabling the organization to maintain optimal system health and performance.	

19	**Manufacturer Authorisation**	The manufacturer authorization letter should be provided specifically in the name of the bidder, authorizing them to supply, install, and support the offered solution directly from OEM to Customers Email	
20	**Local Experience**	The bidder must have past experience of deployment of similar solution in at least 3 Enterprise, Education, Health or government organization in Nepal. Proof of reference documents must be submitted	
21	**Bidder Response**	The bidder is responsible for installation, performance tuning, onsite support during installation phase and configuration to ensure the firewall operates as proposed in the network environment. Should migrate existing firewall policy into new firewall along with the existing network with proper documentation.	

Wireless Access Point's Required Specifications for both National Office and Branch Locations

S No	Specification / Requirement	Compliance (Yes/No)
A	Brand [*To be Mentioned by bidder*]	
B	Model [*To be Mentioned by Bidder*]	
C	Quantity [Refer Annex B]	
D	Type [Wireless Access Point]	
1	The APs should support the 802.11a, 802.11b, 802.11g and 802.11n, 802.11ac and 802.11ax standards.	
2	Simultaneous client support on dual band radio is essential.	
3	Shall provide Min 23 dBm Radio output power for both Radio's.	
4	Should support minimum 2x2:2 or higher MIMO on both radio bands for an aggregate capacity of around 1700 Mbps	
5	The Access points should be Centrally Managed by a full-fledged controller hosted by OEM in cloud. The proposed solution should be quoted with 3 years cloud controller license.	
6	It should have adaptive antenna technology for performance optimization and interference mitigation features. Antenna should provide Extended coverage utilizing multi-directional antenna patterns. Access point to have Polarization Diversity with Maximal Ratio Combining (PDMRC).	
7	Antenna should dynamically choose antenna patterns in real-time environment to establish the best possible connection with every device. Should support at least 50 antenna patterns combinations.	
8	The access point should be able to detect clients that have dual band capability and automatically steer those client to use the 5GHz band instead of the 2.4GHz band.	
9	Antenna should direct the radio signals per-device on a packet-by-packet in real-time to support high device density environments. Should have 3 dBi gain. Antenna operates without the need for device feedback to support devices using legacy standards.	
10	AP should have 1x1Gbps RJ-45 based Ethernet PoE port.	
11	It should have less than 15 Watts power consumption for full functionality including USB port on PoE.	

12	The access point should support IOT based technologies such as Bluetooth, zigbee either inbuilt or using an external usb module.	
13	The access point should support WPA2 and WPA3 enterprise authentication and AES/CCMP encryption. AP should support Authentication via 802.1X and Active Directory.	
14	Implement Wi-Fi alliance standards WMM, 802.11d, 802.11h and 802.11e	
15	Should support the following channelization - 20MHz, 40MHz, 80MHz	
16	Should support min 250 clients per AP or more	
17	AP should be flexible hardware to be deployed as Standalone, Controller-less (Cluster), Controller-based, Cloud-based.	
18	AP should be able to act as sensor for WIPS, Location analytics engine and Network analytics engine.	
19	The access point should include application recognition and control	
20	APs should be site survivable. It should be possible to configure as such if controller goes down, still APs should be able to handle client traffic.	
21	AP should have recovery SSID for easy access to CLI console when AP is unreachable through network.	
22	Shall support 16 SSID's per AP.	
23	Shall support 1 USB port also.	
24	Operating Temperature: 0°C - 40°C	
25	Operating Humidity: 10 % - 95% non-condensing.	
26	The manufacturer authorization letter should be provided specifically in the name of the bidder, authorizing them to supply, install, and support the offered solution directly from OEM to customer's email	
27	Must include POE Injector - 24 Watt with Gigabit port	

Network Switch required specification for branch location

S. No.	Specification Required	Compliance (Yes/No)
1	**Product details - Please specify**	
1.1	Please mention Make, Model No. and Part Code.	
2	**Architecture & Port Density**	
2.1	The Switch should have minimum Twenty-four (24) 10/100/1000Mbps PoE+ RJ45 ports and should have Four (4) 1G/10G SFP+ ports.	

3	**Performance**	
3.1	Switching Bandwidth: The Switch should provide Switching Capacity of 128 Gbps or more.	
3.2	Forwarding Capacity: The Switch should provide Packet Forwarding Capacity of 95 Mpps or more.	
4	**Features**	
4.1	Should support 4K Vlan ID.	
4.2	Should support 16K MAC addresses or more.	
4.3	Should support IP multicast snooping IGMP v1, v2, v3	
4.4	Should support Jumbo Frames (up to 9K bytes)	
5.1	Should support minimum 900 IPv4 routes or more	
5.2	Should support Basic IPv4 and IPv6 Static Routing.	
6	**Security**	
6.1	Should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords.	
6.2	Should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
6.3	Should support IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection.	
6.4	Should support IPv4 and IPv6 ACLs with up to 1K rules per ACL.	
6.5	Should support Flexible Authentication with 802.1x Authentication and MAC Authentication.	
7	**Manageability**	
7.1	Should support manageability using Network Management Software with Web based Graphical User Interface (GUI).	
7.2	Should support Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring.	
7.3	Should support NetFlow or sFlow or equivalent.	
8	**Physical Attributes, Memory, Power Supply and Fans**	
8.1	The Switch should be compatible with 19" Universal rack.	
8.2	The Switch should have minimum 1GB of Memory and minimum 1GB Flash Memory.	

8.3	PoE Power Budget: The Switch should provide a minimum of 195 watts of PoE+ power.	

Meraki License Requirement for Cisco Meraki MS-225-24 and MS120-48.

Device	**Cisco Meraki MS-224**	**Compliance (Yes/No)**
Quantity	Mentioned in Annex B	
CON-ROB-MS22524P	RMA UPGRADE 8X5XNBD Meraki MS225-24P L2Cld-Mngd 24xGigE370W	
LIC-MS225-24P-3YR	Meraki MS225-24P Enterprise License and Support, 3YR	

Device	**Cisco Meraki MS-120**	**Compliance (Yes/No)**
Quantity	Mentioned in Annex B	
CON-ROB-MS12048W	RMA UPGRADE 8X5XNBDMeraki MS120-48 1GL2Cld Md48x GigE Sw	
LIC-MS120-48-3YR	Meraki MS120-48 Enterprise License and Support, 3 Year	

Annex B

Detail of unit of the devices and licenses required based on the location:

Total units of required Network Security Appliance

Location	Address	Required Units
National Office	Sanothimi, Bhaktapur	2
FLC Bharatpur	Gaurijang, Bharatpur, Chitwan	1
FLC Dhangadhi	Dhangadhi -13, Airport Road, Mohanpur, Kailali	1
FLC Itahari	Balgram - 7, Itahari, Sunsari	1
FLC Jorpati	Narayantar -6, Gokarneshwor Municipality, Kathmandu	1
FLC Kavre	Srikhandapur, Panauti, Kavre	1
FLC Lumbini	Siddharthanagar-4, Rupandehi	1
FLC Pokhara	Chorepatan, Pokhara, Kaski	1
FLC Surkhet	Kalagaun, Birendranagar, Surkhet	1
FLC Gandaki	RamBazzar, Pokhara, Kaski	1
EDU Pokhara	Gharipatan, Pokhara-17, Kaski	1
SGH Bharatpur Boys	Tigerchowk, Bharatpur, Chitwan	1
SGH Biratnagar Boys	Biratnagar-13, Morang	1
SGH Biratnagar Girls	Biratnagar-2, Morang	1
SGH Buddhanagar	Buddhanagar, Kathmandu	1
SGH Dhangadi Girls	Dhangadhi - 5, Hasanpur, Kailali	1
SGH Gandaki Girls	Birauta, Pokhara -17, Kaski	1
SGH Lumbini Boys	Siddharthanagar-08, Radhe path, Rupandehi	1
SGH Nepalgunj Boys	Karkandoo, Nepalgunj, Banke	1
SGH Nepalgunj Girls	Belaspur, Nepalgunj,Banke	1
SGH Sanothimi	Sanothimi, Bhaktapur	1
	Total	22

Total units of required Wireless Access Point

Location	Address	Units required
National Office	Sanothimi, Bhaktapur	3
FLC Bharatpur	Gaurijang, Bharatpur, Chitwan	1
FLC Dhangadhi	Dhangadhi -13, Airport Road, Mohanpur, Kailali	2
FLC Gandaki	Rambazar, Pokhara -15, Kaski	2
FLC Itahari	Balgram - 7, Itahari, Sunsari	3
FLC Jorpati	Narayantar -6, Gokarneshwor Municipality, Kathmandu	2
FLC Kavre	Srikhandapur, Panauti, Kavre	5
FLC Lumbini	Siddharthanagar-4, Rupandehi	4
FLC Pokhara	Chorepatan, Pokhara, Kaski	1
FLC Sanothimi	Sanothimi, Bhaktapur	2
FLC Surkhet	Kalagaun, Birendranagar, Surkhet	2
EDU Bharatpur	Gaurijang, Bharatpur, Chitwan	4
EDU Gandaki	Rambazar, Pokhara -15, Kaski	3
EDU Pokhara	Gharipatan, Pokhara-17, Kaski	1
EDU Itahari	Balgram - 7, Itahari, Sunsari	4
EDU Kavre	Srikhandapur, Panauti, Kavre	4
EDU Sanothimi	Sanothimi, Bhaktapur	2
CPT Kavre	Srikhandapur, Panauti, Kavre	1
EET Pokhara	Chorepatan, Pokhara, Kaski	1
SGH Bharatpur Girls	Gaurijang, Bharatpur, Chitwan	3
SGH Bharatpur Boys	Tiger Chowk, Bharatpur, Chitwan	2
SGH Biratnagar Boys	Biratnagar-13, Morang	2
SGH Biratnagar Girls	Biratnagar-2, Morang	1
SGH Buddhanagar	Buddhanagar, Kathmandu	1

SGH Dhangadi Girls	Dhangadhi - 5, Hasanpur, Kailali	1
SGH Gandaki Boys	Rambazar, Pokhara -15, Kaski	1
SGH Gandaki Girls	Birauta, Pokhara -17, Kaski	1
SGH Jorpati Girls	Koteshwor, Kathmandu	3
SGH Lumbini Boys	Siddharthanagar-08, Radhe path, Rupandehi	3
SGH Nepalgunj Boys	Karkandoo, Nepalgunj, Banke	1
SGH Nepalgunj Girls	Belaspur, Nepalgunj,Banke	2
SGH Sanothimi	Koteshwor, Kathmandu	2
	Total	**68**

Total units of required network switches

Location	Address	Required No of Switches
CPT Kavre	Srikhandapur, Panauti, Kavre	1
SGH Jorpati	Koteshwor, Kathmandu	1
EET Pokhara	Chorepatan, Pokhara, Kaski	1
	Total	**3**

Total units of required Fiber equipment

Location	Address	SFP	Fiber and Conduit in meters
CPT Kavre	Srikhandapur, Panauti, Kavre	1 Pair	0
SGH Jorpati	Koteshwor, Kathmandu	1 Pair	200
	Total	**4**	**200**

Total number of required Meraki Licenses to be applied on Meraki dashboard

Cisco Meraki MS-224	**13**
Cisco Meraki MS-120	**1**

Annex C

The technical configurations that need to be applied after the deployment of the devices. Configurations include, but are not limited to:

Network Security Appliance

- Uplink IP Configuration as per provided network design
- Hostname & Device Time synchronized with NTP server
- Default password update for all device accounts
- Disable management console access outside Management VLAN
- Syslog server configuration (IP & port)
- SNMP configuration (collector IP)
- Auto firewall firmware update; coordinate upgrade window
- High Availability (HA) / hot spare configuration
- Scheduled configuration backup & versioning
- Admin account hardening (least privilege, separate read-only accounts)
- Layer 3 outbound rules replication
- Layer 7 / Application-level rules replication
- Content filtering rules replication
- Port forwarding replication if exists
- Inbound firewall logging enabled
- SSL/IPsec client VPN configuration
- Site-to-site VPN with SD-WAN and other peers
- Replication of current group policies
- Two-Factor Authentication (2FA) enabled for login
- VPN encryption protocols enforced (AES-256 or better)
- IDS enabled for signature-based detection
- IPS enabled for inline blocking of known threats
- IPS/IDS rules tuned to minimize false positives
- Threat logging integrated with Syslog and alerting
- Best practice security features enabled (anti-spoofing, DoS protection, rate-limiting)
- Deep packet inspection / advanced threat inspection enabled
- Alerts / email notifications for critical events

- Configure all subnets and VLANs per network design
- Per-port VLAN settings
- DHCP configuration for each subnet
- Replicate fixed/static IP assignments
- MAC binding to restrict network access
- SD-WAN configuration including uplink settings and load balancing
- Traffic shaping and flow preferences (per-user or per-bandwidth)
- QoS configuration per organization requirements
- Uplink statistics and flow preference configuration
- Password expiration enforced
- Password history enforced
- Minimum password length enforced
- Account lockout after defined failed attempts
- Idle session timeout enforced

Wireless Access Point

- Device hostname & location labeling
- Device time synchronized with NTP server
- Default passwords change for all device accounts
- Restrict device management access to dedicated VLAN
- Cloud-based centralized management configuration
- Automated firmware updates via cloud management
- SNMP configuration for monitoring
- Syslog integration for device logs
- Scheduled backup of configuration
- Configure Wi-Fi SSID for official devices
- Certificate-based authentication (EAP-TLS)
- Integration with Intune / Mobile Device Management for automatic profile & certificate deployment
- VLAN mapping for each SSID
- Per-radio band configuration (2.4 GHz / 5 GHz)
- RF optimization features (automatic channel selection, load balancing, band steering)
- Guest network isolation with captive portal (if required)
- Client bandwidth control & QoS configuration

- Rogue AP detection & mitigation
- WPA3 / WPA2 enterprise encryption enforcement
- Integration with RADIUS / Certificate Server for authentication
- Handover of legacy APs to program in-charge
- Detailed network diagram & device configuration documentation
- Alerting / logging for device status & RF anomalies
- High Availability / load balancing of WAPs
- Monitoring client connection statistics & usage
- Physical installation standards: racking, cable management, labelling

***