Terms of Reference (TOR)

Gap Assessment in Network Optimization and Network Security Audit

Dhulikhel Hospital Kathmandu University Hospital (DHKUH)

1. BACKGROUND

Dhulikhel Hospital's critical operations depend entirely on a sophisticated on-premises network infrastructure that supports patient record systems, clinical applications, medical devices, administrative functions, and backup systems.

With the increasing complexity of networked medical equipment, electronic health records (EHR), and integrated hospital systems, there is a need for a comprehensive assessment focusing on both network performance optimization and security vulnerabilities. This will ensure network efficiency, reliability, and capacity utilization while maintaining robust protection against cyber threats.

Additionally, as DHKUH is also an academic institution, its network infrastructure supports digital learning environments, research collaborations, and secure access to academic resources. It is essential to balance clinical operations with the growing academic and research demands on the network while maintaining strong data privacy and security compliance.

2. OBJECTIVES

The primary objective of this assessment is to comprehensively evaluate and enhance the performance and security of the on-premises hospital and academic network infrastructure through network optimization and a thorough security gap assessment.

2.1 Network Optimization

- Measure current network performance metrics including latency, throughput, packet loss, jitter, and bandwidth utilization.
- Analyze traffic patterns, congestion points, and capacity limitations affecting clinical and academic operations.
- Evaluate QoS implementations for critical medical applications, VoIP systems, and real-time patient monitoring.
- Recommend improvements to network architecture, device configurations, and traffic management for enhanced performance.

2.2 Network Security Assessment

- Identify performance gaps, enhance efficiency, strengthen cyber resilience, and ensure alignment with relevant compliance standards (e.g., HIPAA, NIST Cybersecurity Framework, ISO 27001).
- Assess the effectiveness of network segmentation, firewall rules, RBAC implementations, multi-factor authentication, and privileged access management.
- Evaluate IDS/IPS systems, security monitoring, incident response procedures, and threat intelligence integration.
- Ensure adherence to international best practices for on-premises data handling.

3. SCOPE OF WORK

3.1 Network Optimization Components

- **Analysis and Monitoring**: Real-time and historical analysis of network traffic patterns, protocol usage, and bandwidth consumption.
- **Performance Metrics Collection**: Comprehensive measurement of latency, throughput, packet loss, error rates, and network utilization.
- **Capacity Planning Assessment**: Analysis of current usage patterns and future growth requirements for bandwidth and infrastructure.
- **Network Infrastructure Review**: Examination of switch configurations, routing protocols, load balancing, and redundancy mechanisms.

3.2 Network Security Assessment Components

- **Asset Discovery and Inventory**: Complete mapping of routers, switches, firewalls, servers, endpoints, wireless infrastructure, (Future: PACS, and medical/IoT devices.)
- **Vulnerability Scanning**: Automated and manual security assessments of all network components, applications, and configurations.
- **Penetration Testing**: Controlled security testing to identify exploitable vulnerabilities and validate security controls.
- **Network Segmentation Analysis**: Review of network zones, VLANs, access controls, and micro-segmentation implementations.

3.3 Academic and Research Network Considerations

- **Academic Network Segmentation**: Ensure separation of academic traffic (students, faculty, and research) from critical hospital operations to prevent service disruption.
- **E-Learning & Collaboration Platforms**: Review the performance and security of Learning Management Systems (LMS), tele-education tools, and video conferencing systems.
- **Research Data Security**: Assess policies and technical controls for safeguarding sensitive research data, intellectual property, and ongoing study datasets.
- **Bandwidth Allocation**: Review bandwidth utilization and QoS to ensure priority allocation for online classes, examinations, and tele-education sessions without affecting clinical systems.
- **Secure Remote Access**: Recommend secure VPN/remote access solutions for faculty, students, and researchers to connect to institutional resources from off-site locations.
- **Compliance and Data Privacy**: Evaluate compliance with educational data privacy standards and recommend policies for student data protection and secure sharing of research outputs.

3.4 Data Protection and Privacy

- Review data classification and access controls for patient, research, and student data.
- Verify encryption for data at rest and in transit.
- Assess data retention, archival, and secure disposal practices.
- Evaluate compliance with privacy regulations (HIPAA, GDPR, ISO 27001).
- Review audit logs and incident response for data breaches.

4. METHODOLOGY

4.1 Network Optimization Methodology

- Establishment of current performance metrics using SNMP monitoring, flow analysis, and packet capture.
- Deep packet inspection and flow monitoring to understand application usage and bandwidth consumption.
- Identification of congestion points through real-time monitoring and stress testing.
- Predictive analysis for future bandwidth and infrastructure requirements.
- Identification of seamless, high-performance wireless networks for clinical mobility and medical IoT.

4.2 Security Assessment Methodology

- Passive information gathering and network topology mapping.
- Automated scanning using industry-standard tools (OpenVAS, Qualys, etc.) and manual verification.
- Controlled exploitation attempts following OWASP and NIST guidelines.

5. ELIGIBILITY CRITERIA

- At least 10 years of company establishment, with a minimum of 5 years' experience in IT and Security Consulting with a proven record of accomplishment.
- Technical team possessing certifications related to Network and Security.
- Demonstrated knowledge of international security frameworks and regulations.
- Accreditation from recognized international bodies or standards organizations.
- Vendor must be certified as ISO 27001:2013 or ISO 27001:2022 and ISO 9001:2015

6. REQUIRED RESOURCES

Domain Expertise Required from Bidders:

S.N.	Domain Expert	Minimum Certification & Experiences
1	Team Leader	CISA OR CISSP or equivalent, 10+ years relevant experience
2	Network Security Expert	CCNP / Sophos / Fortinet / Palo Alto / NS1 or equivalent, 5 - 7 years relevant experience
4	Cybersecurity Expert	CEH / OSCP / CREST or equivalent, 5+ years relevant experience
5	Skills	Expertise in tools like Wireshark, Nessus, or firewall-specific diagnostics; proficiency in network monitoring tools, expertise in penetration testing methodologies, strong analytical, reporting, and stakeholder communication skills.

7. DELIVERABLES

7.1 Network Optimization Deliverables

- **Network Performance Baseline Report**: Current performance metrics, capacity utilization, and bottleneck analysis.
- **Traffic Analysis Report**: Detailed breakdown of network usage patterns, application performance, and bandwidth consumption.
- **Optimization Recommendations**: Prioritized list of improvements for enhanced performance and capacity.

Deliverables shall also include:

- **Executive Summary:** Strategic overview combining security and performance findings for hospital and academic leadership.
- **Technical Implementation Roadmap**: Phased approach for security remediation and network optimization with timelines and resource requirements.
- **Ongoing Monitoring Plan**: Framework for continuous security and performance monitoring with recommended tools and metrics.

7.2 Security Assessment Deliverables

- **Security Risk Assessment Report**: Comprehensive vulnerability analysis with CVSS scoring and risk prioritization.
- **Penetration Testing Report:** Detailed findings from security testing with proof-of-concept demonstrations.

8. Confidentiality

The selected firm will be required to sign a **Non-Disclosure Agreement (NDA)**. All data, configurations, and reports are the property of **Dhulikhel Hospital Kathmandu University Hospital (DHKUH)** and must not be disclosed to third parties.

9. Tentative Timeline

"This project is a time-bound engagement, expected to be completed within 1–2 months from the kickoff date, covering assessment, analysis, and final reporting. Any additional support for implementation can be negotiated separately, depending on the recommendations of the final roadmap."

Activity	Date
Proposal Submission Deadline	Within a week
Audit Commencement	30 days
Draft Report Submission	One week
Final Report & Presentation	One week

10. REQUIRED DOCUMENTS FROM BIDDERS

- Detailed organization profile.
- CVs of key team members including certifications and relevant experience.
- Copy of company registration certificate.
- Copy of VAT/PAN registration certificate.
- The bidder must submit a minimum of three (3) experience letters demonstrating successful completion of similar projects.
- Tax submission certificate for lates fiscal year.

11. Contact Information

IT Department

Dhulikhle Hospital Kathmandu University Hospital

it@dhulikhelhospital.org