# TENDER

**FOR**

**IT AUDIT SERVICES**

**Logical and Physical Infrastructure Audit**

**SENDING DATE:** 10TH APRIL 2026

**Address:**

Lycee Français Denis Diderot - French School

P.O. Box 47525,

Argwings Kodhek Road,

00100 GPO Nairobi

Kenya

**Tenders shall be emailed to the following emails address:**

tenders@lyceefrancaisnairobi.com

**CLOSING DATE – 17TH APRIL 2026**

*FRENCH VERSION BELOW*

## 1. Purpose of the Assignment

The French School Nairobi invites qualified IT service providers to submit proposals for conducting a comprehensive audit of its information system, covering both logical and physical infrastructure.

The objective of this audit is to deliver a detailed diagnosis, followed by practical and actionable recommendations to enhance performance, security, and scalability of the IT environment.

## 2. Presentation of the Existing IT Environment

The current IT infrastructure includes:

· Desktop computers, monitors, keyboards, and mice
· Laptops and tablets
· 8 servers (on-premise and/or hosted)
· HP printers and 9 leased photocopiers
· Projectors and interactive smartboards
· DSLR cameras
· Audio systems and public address equipment
· PABX system, landline phones, and mobile phones
· Sophos firewall
· 18 managed switches and 19 access points

## 3. Context and Key Challenges

The school operates in the following environment:

· Dual internet connectivity:
  o Primary: Safaricom (140 Mbps)
  o Backup: Liquid Telecom (70 Mbps), managed via Sophos firewall

**- Current Issues Identified:**

· Degraded internet performance
· Slow startup and performance of workstations
· Backup power inverter not functioning during KPLC outages
· Lack of asset tagging and ticketing systems
· Need for proper licensing management (e.g., Microsoft Office)

## 4. Objectives of the Audit

The selected provider will be required to:

1. Assess the overall IT infrastructure (hardware, software, and network) 2. Evaluate system security and resilience
3. Identify weaknesses and risks
4. Recommend improvements aligned with best practices
5. Support the school's strategy to expand digital usage in education

## 5. Scope of Work

### 5.1 Infrastructure Audit

· Assess the condition and capacity of IT equipment (desktops, laptops, printers, servers)
· Conduct a full inventory of network components (switches, routers, cabling) · Evaluate physical infrastructure (server rooms, cabling, power systems)

### 5.2 Systems and Network Audit

· Review configurations of workstations and servers
· Evaluate server performance and specifications
· Analyze network configuration and architecture
· Verify application compliance and licensing
· Assess authentication and authorization mechanisms
· Identify software conflicts and compatibility issues
· Perform vulnerability assessments and penetration testing

### 5.3 Communication Systems

· Evaluate LAN performance, reliability, and coherence
· Assess email and messaging systems
· Analyze internet and telecom connectivity
· Review traffic flows and access management

### 5.4 Security Audit

· Evaluate backup systems and data recovery procedures
· Review business continuity and disaster recovery plans

- Assess physical and logical security measures:
    - Firewalls, antivirus, filtering systems
    - Access control and monitoring
- Review IT governance procedures:
    - Access rights management
    - Logging and monitoring
    - Maintenance processes

## 6. Deliverables

The audit must result in a comprehensive report including:

- Detailed findings and observations
- Full inventory of IT assets
- Network architecture diagram
- Identification of strengths and weaknesses
- Risk assessment and prioritization
- Immediate corrective actions
- Strategic recommendations (technical and organizational)
- Proposed IT security policy

**Timeline:**

- Preliminary report: within 5 working days after start
- Final report: within 5 additional working days

## 7. Duration of the Assignment

- Maximum duration: **10 working days**
- Start date: within **5 days after contract award**

## 8. Submission Requirements

- Mandatory **site visit** prior to submission
- Proposals must include:
    - Technical proposal (methodology, tools, experience)
    - Financial proposal (exclusive of taxes)
- Language: **English required; French is a strong advantage**

## 9. Submission Deadline

Submissions must be sent electronically to: **tenders@lyceefrancaisnairobi.com.** Submission deadline: **17th April 2026 at 17:00 EAT.** Late submissions will be considered non-responsive

## 10. Additional Expectations

The selected provider should demonstrate:

· Proven experience in IT audits (education sector preferred)
· Strong expertise in cybersecurity and network infrastructure
· Ability to deliver clear, practical, and actionable recommendations

**APPEL D'OFFRE**

**AUDIT INFORMATIQUE**

**Audit de l'infrastructure logique et physique**
**Lycée français international Denis DIDEROT**

## 1. Objet de l'Appel d'Offres

Le lycée français international Denis DIDEROT invite les prestataires de services informatiques qualifiés à soumettre des propositions pour réaliser un audit complet de son système d'information, couvrant à la fois l'infrastructure logique et physique.

L'objectif de cet audit est de fournir un diagnostic détaillé, suivi de recommandations concrètes et actionnables afin d'améliorer la performance, la sécurité et l'évolutivité de l'environnement informatique.

## 2. Présentation de l'environnement informatique existant L'infrastructure

informatique actuelle comprend :

- Ordinateurs de bureau, écrans, claviers et souris
- Ordinateurs portables et tablettes
- 8 serveurs (sur site et/ou hébergés)
- Imprimantes HP et 9 photocopieurs loués
- Vidéoprojecteurs et tableaux interactifs
- Appareils photo reflex numériques (DSLR)
- Systèmes audio et équipements de sonorisation
- Système PABX, téléphones fixes et mobiles
- Pare-feu Sophos
- 18 switchs gérés et 19 points d'accès

## 3. Contexte et principales problématiques

L'école fonctionne dans l'environnement suivant :

- **Connectivité Internet double** :
  - Principale : Safaricom (140 Mbps)
  - Secours : Liquid Telecom (70 Mbps), gérée via le pare-feu Sophos

**Problèmes identifiés:**

- Dégradation de la performance Internet
- Lenteur au démarrage et dans l'utilisation des postes
- L'onduleur de secours ne fonctionne pas lors des coupures KPLC
- Absence de système de suivi des équipements et de ticketing

· Gestion des licences (ex. Microsoft Office) insuffisante

## 4. Objectifs de l'audit

Le prestataire sélectionné devra :

· Évaluer l'ensemble de l'infrastructure informatique (matériel, logiciels et réseau) · Évaluer la sécurité et la résilience du système
· Identifier les faiblesses et les risques
· Proposer des améliorations conformes aux bonnes pratiques
· Soutenir la stratégie de l'école visant à développer l'usage du numérique dans l'enseignement

## 5. Périmètre de l'audit

### 5.1 Audit de l'infrastructure

· Évaluer l'état et la capacité des équipements informatiques (postes, serveurs, imprimantes)
· Réaliser un inventaire complet des composants réseau (switchs, routeurs, câblage)
· Évaluer l'infrastructure physique (salles serveurs, câblage, systèmes d'alimentation)

### 5.2 Audit des systèmes et du réseau

· Vérifier les configurations des postes et serveurs
· Évaluer les performances et spécifications des serveurs
· Analyser la configuration et l'architecture réseau
· Vérifier la conformité des applications et des licences
· Évaluer les mécanismes d'authentification et d'autorisation
· Identifier les conflits logiciels et problèmes de compatibilité
· Réaliser des tests de vulnérabilité et d'intrusion

### 5.3 Systèmes de communication

· Évaluer la performance, la fiabilité et la cohérence du réseau local (LAN) · Évaluer les systèmes de messagerie
· Analyser la connectivité Internet et télécom
· Examiner le flux du trafic et la gestion des accès

### 5.4 Audit de sécurité

· Évaluer les systèmes de sauvegarde et les procédures de restauration
· Examiner les plans de continuité et de reprise après sinistre

Évaluer les mesures de sécurité physique et logique :

- o Pare-feu, antivirus, systèmes de filtrage
- o Contrôle des accès et supervision

· Examiner les procédures de gouvernance IT :

- o Gestion des droits d'accès
- o Journalisation et supervision
- o Processus de maintenance

## 6. Livrables

L'audit doit produire un rapport complet comprenant :

· Constats et observations détaillés
· Inventaire complet du parc informatique
· Schéma d'architecture réseau
· Identification des forces et faiblesses
· Évaluation et priorisation des risques
· Actions correctives immédiates
· Recommandations stratégiques (techniques et organisationnelles)
· Politique de sécurité informatique proposée

**Calendrier:**

· Rapport préliminaire : sous 5 jours ouvrés après le début de l'audit
· Rapport final : sous 5 jours ouvrés supplémentaires

## 7. Durée de la mission

· Durée maximale : **10 jours ouvrés**
· Démarrage : dans les **5 jours suivant l'attribution du contrat**

## 8. Modalités de soumission

· ***Visite du site obligatoire*** avant soumission
· Les offres doivent inclure :

- o Offre technique (méthodologie, outils, expérience)
- o Offre financière (hors taxes)

· Langue : anglais requis, français fortement recommandé

## 9. Date limite de soumission

Les candidatures doivent être envoyées par voie électronique à l'adresse suivante : tenders@lyceefrancaisnairobi.com. Date limite de dépôt des candidatures : le 20 avril 2026 à 17 h 00 (heure d'Afrique de l'Est). Les candidatures reçues après cette **date ne** seront pas prises en compte.

## 10. Exigences supplémentaires

Le prestataire sélectionné doit démontrer :

· Expérience avérée en audit informatique (secteur éducatif préféré)
· Expertise solide en cyber sécurité et infrastructure réseau
· Capacité à fournir des recommandations claires, concrètes et actionnables