

**TDR POUR RENFORCEMENT DE CAPACITE ET FORMATION DE BASE DES AGENTS DE LA DRSI EN CHARGE DE LA GESTION DU RESEAU INTRANET DE L'UL ET SUPPORTS AUX UTILISATEURS**

**1. CONTEXTE ET JUSTIFICATIONS**

L'université de Lomé, pour répondre de façon efficace à ses activités, de gestion des étudiants, des inscriptions, des cours, des activités connexes liées à la formation et au besoin de contrôle et d'évaluation, s'est dotée d'un système d'information reposant sur des infrastructures informatiques et d'une Direction des Ressources et Supports Informatiques (DRSI). Cette Direction repose sur des divisions qui gèrent les ressources informatiques et réseau avec des accès à l'INTERNET de l'Université de Lomé.

Le réseau local est un vaste réseau INTRANET en fibre optique avec des redondances, disposant des serveurs, de plusieurs sous réseaux (pour les différentes structures de l'UL et les étudiants) et des points d'accès sans fil centralisés sous le contrôle et la supervision d'une équipe technique (Division Système d'Information et Division Maintenance et Réseau). Ces deux divisions sont appuyées pour les besoins de développement par une Division Développement d'application.

Pour les besoins des solutions durables, d'extension du réseau INTRANET et de sa supervision dans une veille technologique, la DRSI a besoin de renforcer les compétences des équipes techniques sur les équipements installés sur le réseau et des solutions de filtrage, de supervision et de gestion de ses bandes passantes.

Pour ce faire la nécessité de commander un certain nombre de formations pour renforcer les compétences du personnel des différentes équipes de support et de gestion du réseau INTRANET de l'Université s'impose.

Ces formations sont déclinées en 5 composantes qui pourront être offertes par une structure ou plusieurs structures affiliées devant permettre d'atteindre les objectifs fixés.

**2. OBJECTIF GENERAL**

Il s'agit de former les membres des différentes équipes identifiés au nombre de 7 sur les différentes solutions existantes et à compléter sur l'INTRANET de l'Université pour répondre au besoin d'extension des services et de gestion du réseau au niveau sécuritaire, de gestion de la bande passante, de redondance et de qualité de service de façon pérenne et évolutive.

**3. OBJECTIFS SPECIFIQUE**

Il s'agira pour la structure identifiée à former les différents acteurs de la DRSI sur les 5 compétences suivantes :

**3.1. FORMATION SUR L'INFORMATIQUE DANS LES NUAGES**

Cette formation devra permettre de renforcer les compétences des différents acteurs à :

- Évaluer les apports du cloud computing pour l'Université

- Découvrir les principes clés du cloud computing et ses différents modes de déploiement
- Maîtriser les étapes clés d'un projet de mise en place d'un cloud privé
- Gérer la sécurité du cloud computing

La durée prévisionnelle de cette formation sera de : 20 heures

### **3.2. FORMATION SUR LA CONFIGURATION DES SWITCH ET ROUTEUR MIKROTIK**

Cette formation devra permettre de renforcer les compétences des différents acteurs à maîtriser les différentes techniques sur les équipements MIKROTIK existant dans le réseau Intranet de l'UL avec :

- Le Switching et Management des Ports,
- La configuration du Routage statique et dynamique
- La configuration Inter VLANs,
- La Configuration du Bridge, du Firewall sur l'équipement MIKROTIK existant,
- La configuration et gestion de la qualité de service ou du QoS

La durée prévisionnelle de cette formation sera de : 24 heures

### **3.3. FORMATION CISCO (FIREWALL, EQUILIBRAGE DE CHARGE ET QoS)**

Cette formation devra permettre de renforcer les compétences des différents acteurs à maîtriser les différentes techniques sur :

- La configuration protocole de routage statique et dynamique
- La construction des topologies commutées redondantes
- Le filtrage et sécurisation du cœur du réseau
- L'installation et la configuration du QoS,
- La gestion des bandes passantes selon le besoin réel des différents réseaux connecté au cœur du réseau.

La durée prévisionnelle de cette formation sera de : 24 heures

### **3.4. FORMATION SUR LA CONFIGURATION DU PEPLINK**

Cette formation devra permettre de renforcer les compétences des différents acteurs à maîtriser les différentes techniques sur l'équipement Peplink installé avec nécessité de faire :

- L'installation et la configuration des Routeurs et réseaux des différents sites interconnectés au réseau du cœur
- La configuration et l'optimisation d'un réseau Multi-WAN
- La configuration du Load Balancing Intelligent.

La durée prévisionnelle de cette formation sera de : 20 heures

### 3.5. FORMATION SUR LE LOGICIEL DE GESTION ET SUPERVISION DU RESEAU ET DE DETECTION D'INTRUSION

Cette formation devra permettre de renforcer les compétences des différents acteurs sur :

- les risques encourus au niveau des réseaux et des serveurs du cœur du réseau et des différentes branches connectées, et d'être capable de mettre en œuvre des moyens de sécurisation adaptés et à identifier,
- la détermination des facteurs de risques, les périmètres de risque, les acteurs, et de trouver les outils de prévisions et de protection adaptées,
- la détection des intrusions de niveau 2 et 3, de même que les attaques physiques, logiques, applicatives, etc.
- La protection des commutateurs d'accès, au niveau sans-fil, au niveau IP, protection des attaques logiques et applicatives,
- La sécurisation des accès distants, et l'établissement des connexion distantes (VPN, le choix cryptographique, VPN IPsec, VPN SSL, le NAC, etc.)

La durée prévisionnelle de cette formation sera de : 24 heures

#### 4. RESULTATS ATTENDUS

Les résultats attendus à l'issu de ces différentes formations sont essentiellement l'atteinte des différents objectifs spécifiques des 5 formations identifiées.

Ce qui permettra d'avoir un vivier de personnel disposant non seulement des compétences essentielles sur la gestion du réseau INTRANET de l'UL, mais aussi de disposer d'un nombre d'acteurs avec des compétences étendues transversales sur différents aspects pouvant être partagés reproduits pour d'autres membres à venir. Ceci permettra d'avoir toujours du personnel sur qui compter en cas de problème et ayant une vision globale sur toutes les fonctionnalités du réseau existant et de son évolution. En cas d'absence ou d'indisponibilité d'un acteur, il y aura toujours une compétence pour répondre au besoin des utilisateurs à travers le groupe WhatsApp et support helpdesk existant.

#### 5. FORMATION PRELIMINAIRE

En prélude à la formation sur les renforcements de capacité énumérés dans les **rubriques 3.1 à 3.5**, Il est demandé qu'une formation initiatique se fasse pour la mise à niveau des participants pour 40 heures suivant le tableau 1.

Cette formation initiatique est constituée uniquement des introductions à chacun des modules de formation et permettra non seulement de vérifier les compétences de base mais aussi de donner des supports de mise à niveau et les supports nécessaires pour l'appropriation des modules de formations à venir et qui doivent être très pratiques sur des équipements réels utilisés dans la production ou existant sur le réseau Intranet de l'Université.

Cette formation initiatique sera suivie plus tard au plus deux (02) mois de la formation pratique ou d'approfondissement.

**Tableau 1 : Rubriques de la formation initiale de mise à niveau**

N°	Les modules de formation	Volume horaire prévisionnel
1	Module-1: Formation Initiatique sur le Cloud Computing	5 heures
2	Module-2: Formation Initiatique sur la Configuration des Commutateurs et Routeurs MikroTik	15 heures
3	Module-3: Formation Initiatique CISCO – (Firewall, Load-Balancing et QoS)	5 heures
4	Module-4: Formation Initiatique sur la Configuration et la Gestion des Equipements PEPLINK	5 heures
5	Module-5: Formation Initiatique – Configuration et Utilisation d'un Logiciel de Supervision Réseau et d'un Logiciel de Détection d'Intrusion	5 heures
6	Module-6: Formation Initiatique – Configuration et Gestion de la Plateforme de Cours en Ligne MOODLE	5 heures
<b>Volume horaire Total Prévisionnel</b>		<b>40 heures</b>

