Règlement de l'utilisation du réseau RNU

1. La présente Charte déontologique définit les règles d'usage qui s'imposent à tout utilisateur du Réseau National Universitaire, nommé ci-après RNU[1] dont la gestion revient au Centre de Calcul El Khawarizmi (CCK) Fournisseur de Services Internet pour les institutions d'enseignement supérieur et de recherche.

2. Le RNU est un réseau qui, par nature, recèle des risques dont le signataire est informé. Il est utilisé sous la responsabilité du signataire.

3. Le signataire, au nom des utilisateurs de son/ses site(s)[2] ayant accès au RNU, s'engage à veiller à se conformer à la présente charte et plus précisément à :

- une utilisation à des fins strictement professionnelles conforme à la finalité du RNU : enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique. Les activités d'administration et de gestion des établissements d'enseignement, de recherche ou de développement sont assimilées à la recherche ou à l'enseignement.
- une utilisation rationnelle des ressources du RNU de manière à éviter toute consommation abusive de ces ressources en limitant l'utilisation d'applications consommatrices de ressources de réseau (chat, diffusion de vidéo/son …).
- une utilisation loyale des ressources du réseau RNU en prévenant et s'abstenant de toute utilisation malveillante destinée à perturber ou porter atteinte au RNU.
- une utilisation des ressources et services du RNU limitée à la communauté de l'enseignement supérieur : enseignants, chercheurs, développeurs, étudiants et administratifs. Ne pas donner accès, à titre commercial ou non, rémunéré ou non, au réseau RNU à des tiers non autorisés sans l'accord préalable du CCK.
- une licité des données véhiculées et mises à disposition sur le RNU et ce, au regard des lois qui leur sont applicables notamment le décret n°97/501 du 14 Mars 1997 relatif à l'usage de l'Internet à des fins professionnelles et aux mesures générales émises et actualisées par l'ATI (Agence Tunisienne d'Internet).
- une mise en oeuvre des ressources techniques et humaines requises pour assurer la bonne gestion du réseau interne de l'institution et un niveau permanent de sécurité conforme à l'état de l'art , aux règles en vigueur dans ce domaine et aux recommandations du CCK (Voir Annexe1 : Stratégie de mise en place d'une politique de gestion et de sécurité des réseaux locaux au sein des institutions universitaires et Annexe 2 : Cahier des charges pour une connexion à

[1] L'expression 'RNU' désigne l'ensemble des réseaux des institutions d'enseignement supérieur et de recherche connectés au réseau Internet via le Centre de Calcul El Khawarizmi (CCK) .

2 Le site du signataire désigne le site à l'intérieur duquel toutes les entités (bâtiments, locaux, etc…) reliées directement ou indirectement au RNU relèvent de la personne morale représentée par le signataire de la présente charte.

Internet via le RNU) et ce pour prévenir les agressions éventuelles à partir ou par l'intermédiaire de son/ses Sites.

4. Le signataire de la charte est informé et accepte expressément que le CCK procède à des contrôles permanents de la bonne utilisation du RNU et qu'en cas de manquement de l'utilisateur à ses obligations et ses responsabilités telles qu'énoncées ci-dessus ou, le cas échéant, à la demande des autorités, le CCK puisse suspendre l'accès de son/ses site(s) au réseau.
5. Le signataire de la présente charte accepte que le CCK prenne des mesures d'urgence, y inclus la décision de limiter ou d'interrompre temporairement pour son/ses site(s) l'accès au RNU pour préserver la sécurité en cas d'incident dont le CCK aurait connaissance. Ces mesures seront toutefois :
   - accompagnées dans les meilleurs délais d'un dialogue avec le correspondant de la Gestion et de la Sécurité[3] du ou des Site(s) concerné(s) ;
   - et ne pourront être mises en oeuvre que dans le cadre d'une procédure approuvée par les responsables sécurité du CCK et sous réserve de leur faisabilité technique et juridique ;

6. Le signataire de la présente charte est informé et accepte que le CCK puisse à tout moment modifier la présente Charte notamment pour tenir compte des évolutions législatives qui peuvent intervenir dans ce domaine; les modifications lui seront notifiées périodiquement.

7. Le signataire de la présente charte , représentant du ou des site(s)

   Identification du et des site(s)
   Adresse :

   reconnaît avoir pris connaissance de la présente Charte déontologique du RNU et de ses annexes et s'engage à la **respecter et à la faire respecter** par tous les utilisateurs relevant de son/ses site(s) et raccordés au RNU et **désigne comme Correspondant technique de la gestion du réseau local et de la sécurité** :

   Nom, Prénom :
   Adresse Electronique :
   Téléphone :
   Télécopie :

Le Signataire :
Nom, Prénom :
Titre :
Adresse élèctronique :
Date :
Téléphone :
Télécopie :
Lu et approuvé
……..

Le Centre de Calcul El Khawarizmi

[3] Le 'Correspondant sécurité' est une personne désignée par le signataire qui doit disposer de tous les pouvoirs opérationnels nécessaires pour intervenir efficacement et dans les meilleurs délais , en cas d'incident de sécurité tant au niveau de la connexion du ou des sites agréés du signataire que sur les éventuelles connexions directes vers d'autres sites.

ANNEXE1 : Stratégie de mise en place d'une politique de gestion et de sécurité des réseaux locaux au sein des institutions universitaires

Face à l'évolution rapide de l'Internet et à la vulgarisation des Nouvelles Technologies de l'Information et de la Communication, et face à l'apparition de nouveaux besoins, une meilleure organisation et administration du réseau local de l'institution prenant en compte l'aspect sécurité s'impose.

En tant que fournisseur de services Internet, le CCK s'engage à connecter chaque institution universitaire à l'Internet et à fournir les différents services tels que la messagerie, la navigation sur le web, l'hébergement des sites web , etc.
Le CCK est tenu de faire respecter la stratégie nationale de sécurité informatique du réseau. Dans ce cadre, il est responsable de la sécurité du Réseau National Universitaire (RNU) (jusqu'au point d'arrivée de la ligne spécialisée aux institutions à savoir le routeur)

La sécurité à l'intérieur de l'institution relevant de la compétence de celle-ci , elle est tenue de sécuriser son réseau local moyennant la désignation d'un responsable se sécurité qui veille à la mise en place de la stratégie de sécurité décrite ci dessous.

1. L'institution universitaire doit désigner un responsable du réseau de nationalité tunisienne ayant au moins de technicien supérieur en informatique pour la gestion et la maintenance du réseau local et du parc informatique.

2. Le responsable de sécurité doit structurer le réseau local de l'institution d'une manière à ne pas connecter les postes critiques d'administration (gestion des examens, des notes, etc.) directement au réseau Internet **sans aucune mesure de sécurité**.

3. Le responsable de sécurité doit procéder à l'installation d'une solution anti-virale sur tous les postes du réseau et veiller à la mise à jour de l'anti-virus et à la désinfection régulière des postes. En cas d'attaque virale, il est conseillé de déclarer l'incident au près du service de sécurité du CCK.

4. Le responsable de sécurité doit procéder à la mise à jour du système d'exploitation (Windows ou linux) sur tous les postes (service pack, patch de sécurité) disponibles sur les sites des éditeurs.

Dans le cadre de la stratégie de sécurité du RNU et de l'amélioration de l'accès à Internet, le CCK s'engage à aider les institutions dans la sécurisation de leur réseau en particulier à l'installation d'un serveur Proxy. Ce serveur Proxy n'est pas une solution finale. Il permet d'améliorer la sécurité du réseau vis à vis de l'extérieur et d'améliorer les débits et constitue certes une étape vers une meilleure sécurité.

- Le serveur Proxy améliore le débit Internet de l'Institution en faisant office de cache. Il masque également les adresses IP de l'extérieur.
- Le serveur Proxy est configuré avec un noyau Firewall (Coupe-feu) du type iptables. Des règles d'accès ont été implémentées pour permettre à tout poste connecté au Proxy de bénéficier des services Internet les plus usuels tels que HTTP, HTTPS, DNS, ICMP, SMTP, POP, FTP, Telnet et SSH.
- Des règles d'accès interdisent également l'accès de tout poste externe à l'institution au réseau derrière le Proxy.
- Le serveur Proxy permet à l'administrateur de gérer les comptes nominatifs créés obligatoirement par le CCK au profit des enseignants et étudiants pour les besoins d'enseignement et de recherche. Ceci a pour objectif de responsabiliser les internautes des institutions et de gérer les droits d'accès des utilisateurs aux services de l'Internet (par plage d'adresses IP, par plage horaire, etc).
- **Les fichiers log générés par le proxy permettent de relever les différents accès aux sites Internet de tous les utilisateurs authentifiés par le proxy**.

5. Le CCK assiste à l'installation et la configuration du système d'exploitation Linux, du Proxy Squid et d'un firewall iptables.

6. L'institution réserve un ordinateur avec des caractéristiques minimales (disque dur: 40 Go, mémoire: 512 Mo, processeur: 1 Ghz, deux cartes réseaux compatibles linux, un graveur de CD pour la sauvegarde).

7. Le responsable de gestion et de sécurité de l'institution a les privilèges d'administration du serveur Proxy, il est amené à faire des sauvegardes et à gérer les problèmes de disfonctionnement.

8. Le CCK a le droit de regard sur le serveur Proxy, les échanges via le réseau peuvent être analysés et contrôlés à tout moment par le personnel du service sécurité du CCK.

9. L'institution est appelée à exploiter, au besoin, les fichiers log pour déceler toute anomalie d'utilisation de l'Internet au niveau de l'institution et de la signaler au service de sécurité du CCK.

10. Le responsable de sécurité de l'Institution est tenu d'effectuer des sauvegardes régulières des fichiers de configuration et des fichiers de logs du serveur Proxy.
    - La sauvegarde des fichiers de configuration est journalière et doit s'étaler sur une semaine.
    - La sauvegarde des fichiers de logs est mensuelle. L'institution est tenue de remettre les fichiers logs au CCK mensuellement et à la demande.

11. Le responsable de gestion et de sécurité doit veiller à la synchronisation de l'heure système du serveur proxy avec un serveur de temps.

12. Tous les utilisateurs de l'institution s'engagent à ne pas apporter volontairement des perturbations au bon fonctionnement du serveur Proxy et du réseau que ce soit par des

manipulations anormales ou par l'introduction de logiciels parasites connus sous le nom générique de virus, Chevaux de Troie , bombes logiques, etc…

13. L'institution est appelée à informer ses utilisateurs des règles de bon usage citées ci dessous :
    - Tout utilisateur est responsable de l'usage du serveur Proxy et du réseau auquel il a accès. Il a aussi la charge de contribuer à la sécurité générale.
    - L'utilisateur s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des moyens dont il a l'usage.
    - L'utilisateur est le seul responsable de son compte. Il ne doit pas quitter le poste de travail utilisé sans se déconnecter.
    - L'utilisateur ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité.
    - L'utilisateur doit signaler au responsable de l'institution toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.

14. Le CCK offre à l'institution un service d'assistance, de conseil, de formation et d'information à travers le compte info@cck.rnu.tn.

ANNEXE 2 : Cahier des charges pour une connexion à Internet via le RNU

Le Centre de Calcul El Khawarizmi CCK en tant que fournisseur de services Internet pour les institutions universitaires et opérateur du RNU (réseau national universitaire), assure 24h/24 et 7jours/7 le bon fonctionnement des services RNU et Internet.
L'utilisation de ces services doit être conforme à la charte déontologique du RNU en s'abstenant de toute utilisation abusive ou frauduleuse.

Pour chaque institution universitaire désirant se connecter à Internet via le RNU, il est nécessaire de :

1. Installer un onduleur pour éviter les éventuelles pannes du secteur STEG et protéger les équipements informatiques notamment le modem, le routeur, les switchs et les serveurs.
2. Protéger les équipements de connexion (le modem, le routeur et les switchs) dans des armoires informatiques et les garder sous tension de façon continue.
3. Installer un climatiseur dans la salle des équipements informatiques et de connexion
4. S'assurer que le câblage informatique et la prolongation de la ligne spécialisée soient conformes aux normes internationales de l'UIT et réalisés par une société agréée par le ministère des technologies de communication .
5. Mettre en place en collaboration avec le CCK un serveur proxy par segment réseau (un pour les étudiants, un pour les enseignants, les chercheurs et les développeurs et un troisième pour les services administratifs)
6. Installer un antivirus mis à jour et bien configuré sur tous les postes du réseau local de l'institution universitaire
7. Désigner un responsable technique de gestion et de sécurité

Rôle du responsable technique de l'institution

Chaque institution universitaire doit désigner un responsable technique qui gère les différents équipements actifs et passifs du réseau local de l'institution notamment le serveur proxy, le modem et le routeur. Dans ce cadre, il doit :

1. maintenir un état mis à jour régulièrement (avec précision des dates de modification) des adresses IP officielles et privées utilisées dans l'institution. Une copie de l'état des adresses IP officielles doit être remis au CCK
2. avoir une copie de la fiche technique de l'institution
3. gérer le modem et le routeur, le CCK peut lui donner le mot de passe de premier niveau du routeur qui lui permettra de vérifier l'état de la ligne
4. être l'intermédiaire entre les utilisateurs (enseignants et étudiants) et le CCK
5. veiller à la sécurité informatique du réseau local conformément à la stratégie de mise en place d'une politique de sécurité au sein des institutions universitaires

Il est à noter que les adresses IP officielles sont strictement réservées aux équipements de connexion (routeur, switchs), aux serveurs d'applications (serveur Proxy, serveur FTP, etc) et aux postes de travails utilisés pour l'accès à des services particuliers. L'accès aux serveurs d'applications doit être

sécurisé et leur utilisation doit être strictement réservée aux fonctions attribuées (pas de navigation à partir de ces serveurs).

Procédure de diagnostic d'un dysfonctionnement

Cette procédure doit être appliquée par le responsable technique de l'institution qui est la seule personne habilitée à adresser des réclamations à propos de la connexion Internet de l'institution aussi bien auprès du CCK qu'auprès de Tunisie Telecom

Le CCK assure en permanence 7jours/7 un suivi des connexions Internet des institutions universitaires à l'aide d'outils logiciels et humains. Toutefois, le CCK ne considère une institution donnée comme présentant une panne que lorsque le responsable technique de celle ci fait une réclamation auprès du service d'assistance technique du CCK. Ce dernier aide le responsable technique à effectuer un diagnostic précis et rapide de la panne.

En cas de perte de connexion Internet, le responsable technique doit effectuer les tests suivants à partir d'une machine ayant une adresse IP officielle (toutes les adresses IP mentionnées ci dessous sont contenues dans la fiche technique de l'institution) :

1. ping @ip du routeur (permet de tester la connectivité entre le poste client et le routeur)
2. tracert @ip Serveur DNS (permet de tracer le chemin du poste client vers la destination)

Si la réponse au premier test est négative, alors la connexion entre le routeur et le réseau local est défectueuse. Le responsable technique doit vérifier le réseau local, les causes pouvant être diverses (un câble débranché, un switch éteint, routeur éteint). Pour les problèmes locaux; l'institution est responsable du rétablissement de la connexion; néanmoins le responsable technique peut demander l'aide du CCK.

Si la réponse au premier test est positive, alors le routeur est joignable à partir du réseau local, la cause de la perte de connexion Internet peut être

- soit la LS du client,
- soit un problème au niveau du backbone national pour les liaisons via le backbone
- soit un problème au niveau du CCK
- ou encore entre le CCK et ses partenaires à savoir l'ATI et/ou le backbone .

Pour mieux localiser le problème, le responsable technique doit appeler le service assistance technique du CCK après avoir effectué le deuxième test et vérifié l'état du modem. Les résultats des deux tests doivent être communiqués au CCK.

Pour les problèmes de connexion physique (LS), le client doit réclamer lui même la panne à TT (service 1115). Le CCK peut aider le client à suivre la panne auprès de TT pour assurer un rétablissement rapide de la connexion.

Pour les problèmes au niveau du CCK ou encore en aval de ce dernier, le CCK déploie tous ses moyens pour rétablir la connexion dans les plus brefs délais.