UNIVERSITE DE LA REUNION
Responsable de la sécurité du système d'information

Politique de Sécurité Interne

OBJECTIF

La Politique de Sécurité Interne (PSI) s'applique au sein de l'université (Moufia), à tous les sites périphériques (IAE, IUT, IUFM, Campus du Tampon et site du PTU) et de fait, à tous les usagers de ces campus (Etudiants et Personnels).
Toutes les règles sont impératives, en cas de problème (suspicion de courrier frauduleux, détection d'intrusion non autorisée sur un poste informatique, virus, …), le RSSI (Responsable de la Sécurité du Système d'Information) et ses correspondants doivent être contactés immédiatement.

Organisation et contrôle de la SSI

Le RSSI est monsieur Laurent PEQUIN

Le RSSI-Suppléant est monsieur Matthieu BANNIER

Le Correspondant Informatique et Libertés (CIL) est monsieur Thierry BRUGNON

Ces acteurs ont pour missions de faire respecter la PSI, de contrôler l'application des règles de la PSI et de réaliser un compte rendu au Président en cas de problème.

L'autorité Qualifiée de la Sécurité du Système d'Information (AQSSI) est le Président de l'université de la Réunion : Pr. Mohamed ROCHDI

RÈGLES DE SÉCURITÉ

Sécurité du Personnel

Après toute phase de recrutement (CDD, CDI, Mutation, Recrutement sur Concours), le nouveau personnel doit être sensibilisé et doit signer la charte d'utilisation des moyens informatiques et la remettre au RSSI.
En cas de changement interne d'un correspondant SSI, une formation doit lui être dispensée immédiatement.

Sécurité des biens physiques

- Un cahier de bord (journaux, logs) est mis à jour dès qu'une opération est réalisée sur un équipement de sécurité comme le firewall ou le serveur proxy d'accès à Internet (cf. la politique de gestion des journaux informatiques)
- La connexion de tout matériel étranger à l'université est interdite sur un ordinateur ou le réseau (téléphone, PDA, clé USB, portable, périphérique)
- La connexion d'un ordinateur étranger (appartenant à un étudiant ou un personnel) à l'université est autorisée dans le seul réseau du portail captif (WiFi)
- L'accès aux ordinateurs de l'université est réglementé et limité selon la configuration mise en place par l'informaticien de composante (salle libre service étudiant, ordinateur de laboratoire, ordinateur administratif). Cette configuration ne doit pas être contournée par quelque moyen que ce soit
- Les ordinateurs portables doivent êtres placés dans une armoire fermée à clé ou attachés à un bureau avec un câble en acier de type Keysington (à clé ou à code)
- Les matériels informatiques (visioconférence, ordinateurs) doivent être référencés et étiquetés

- L'installation et la diffusion de logiciels autres que ceux fournis par le service informatique sont interdites
- Seul un administrateur est autorisé à installer un logiciel sur un poste, les licences personnels étant proscrites
- Tout utilisateur est responsable de son ordinateur et ce dernier doit veiller à la présence d'un antivirus sur son ordinateur

Sécurité de l'information

- Les utilisateurs sont responsables des informations qu'ils manipulent
- Les utilisateurs doivent sauvegarder leurs données et veillent à ne pas porter atteinte à l'intégrité du système (virus, cheval de Troie, intrusion volontaire non autorisée)
- Pour le traitement des informations nominatives, le responsable CNIL de l'Université est l'interlocuteur privilégié.
- Les logs (traces d'activités) des serveurs sont conservés 6 mois
- L'utilisateur ne doit jamais être administrateur de son ordinateur
- L'accès au système d'information doit se réaliser après une procédure d'authentification (login et mot de passe)
- Les paramètres de connexion (paire login ET mot de passe) sont personnels et ne doivent ni être écrites, ni communiqués à un tiers, même de l'équipe informatique
- Un écran de veille doit être automatiquement activé en cas de non utilisation de l'ordinateur pour une période dépassant 15 minutes
- L'utilisateur doit activer son écran de veille (forcer) ou se déconnecter de sa session s'il quitte son bureau
- L'envoi de pièce jointe par messagerie est limité au strict nécessaire
- En cas de virus, tout événement doit être signalé à l'informaticien de composante et au RSSI
- Toute demande d'accès au réseau interne par l'Internet doit obligatoirement passer par le VPN, activé par moncompte.univ-reunion.fr
- La connexion au réseau Skype est fortement déconseillée depuis un poste utilisateur de l'université