



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

Charte d'utilisation des ressources informatiques à l'université de la Réunion

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
10/09/09	Mise à jour du document	Laurent PEQUIN (RSSI)	En cours
05/03/09	Rédaction du document	Laurent PEQUIN (RSSI)	Validé

Table des matières

1.Objectif.....	4
2.Définitions de termes.....	4
Moyens Informatiques.....	4
Services Internet	4
Utilisateurs	5
Compte	5
3. Conditions générales d'utilisation.....	5
4. Obligations des utilisateurs.....	6
4.1. Règles générales.....	6
4.2. Préservation des matériels et locaux.....	6
4.3. Pénétration non autorisée dans les moyens informatiques.....	6
4.4. Utilisation des comptes et des dispositifs de contrôle d'accès.....	6
5. Charte éditoriale.....	7
6. Rôle du CRI.....	8
7. Modification et altération des moyens informatiques.....	8
8. Conséquences des manquements à la charte et poursuites.....	9
8.1. Responsabilité des utilisateurs.....	9
8.2. Mesures applicables par les responsables informatiques.....	10
8.2.1. Mesures d'urgence.....	10
8.2.2. Mesures donnant lieu à information.....	10
8.2.3. Mesures soumises à autorisation du directeur ou responsable du service.....	10
8.3. Sanctions disciplinaires.....	10
8.4. Poursuites civiles et pénales.....	10

1. Objectif

Ce document est avant tout un code de bonne conduite afin de sensibiliser aussi bien le personnel que les étudiants sur les attitudes à adopter face à l'outil informatique.

Un point juridique rappellera la responsabilité des utilisateurs et de l'administration qui garantie un usage correct des ressources informatiques et des services Internet. Ce point mettra notamment l'accent sur les sanctions opposables aux éventuels contrevenants.

Cette charte est un élément à considérer comme faisant partie intégrante du règlement intérieur de l'Université. La présente charte détermine les conditions d'utilisation et d'accès aux ressources informatiques de l'Université.

Tout étudiant qui s'inscrit à l'Université signe implicitement l'acceptation des termes de la présente charte.

L'acceptation de cette charte est également implicite pour les personnels travaillant à l'Université.

2. Définitions de termes

Moyens Informatiques

Nous entendrons par moyens informatiques :

- les serveurs
- stations de travail (ordinateurs)
- postes de consultation
- les réseaux internes et externes de l'Université de la Réunion (réseau filaire, et réseau aérien type Wi-Fi)
- les micro-ordinateurs des services, laboratoires, instituts, centres, UFR
- l'ensemble du parc logiciel
- les bases de données
- des produits multimédias ou des périphériques affectés au fonctionnement des éléments décrits.

Sont également considérés comme moyens informatiques, les ressources extérieures accessibles par l'intermédiaire des réseaux de l'Université de la Réunion et notamment le réseau RENATER.

Services Internet

la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses :

- Web
- messagerie électronique
- forum
- ...

Utilisateurs

Nous définissons un utilisateur comme étant une personne ayant accès (restreint ou non) à certaines ressources informatique. Ceci inclus :

- les étudiants
- les enseignants
- les chercheurs
- les personnels administratifs ou techniques
- les hébergés
- les invités

Compte

Un Compte définit la connexion à des ressources permettant d'avoir un espace disque, une adresse e-mail, et d'accéder aux logiciels correspondant à la fonction exercée ou à l'enseignement suivi.

De part la présente charte, l'Université de la Réunion s'engage à établir un périmètre d'application visant à assurer la :

- Protection du personnel et des étudiants (art. 8 de la convention européenne des Droits de l'Homme, art. 9 du Code Civil, art. 226-22 du Code Pénal qui assimile la divulgation d'informations privées à un délit)
- Protection des systèmes d'information informatisés (Loi « Informatique et Libertés » du 6-1-78)
- Protection des logiciels (L. 335-1 à L. 335-8 du Code de la Propriété Intellectuelle)
- Protection des données (art. 226-17 du Code Pénal – Obligation de sécurité)
- Protection des informations confidentielles (art. 226-22 du Code Pénal)
- Protection du Secret des correspondances (art. 226-15 al.2 du Code Pénal)
- Protection de l'ordre public et la sécurité des personnes (Protection des mineurs par l'art. 227-23 du Code Pénal et Protection de la dignité humaine art. 227-24 du Code Pénal)

3. Conditions générales d'utilisation

L'utilisation des moyens informatiques est limitée au strict cadre et aux seuls besoins de l'activité et de la vie universitaire. Toute autorisation et détention de compte prend fin le jour même de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée et toute persistance des données au delà de cette date incombe à l'utilisateur.

Cependant, une dérogation implicite est donnée afin d'accorder la nécessité de disposer d'une « vie privée résiduelle »

Toute autre utilisation des moyens informatiques dépassant le cadre de l'activité de l'utilisateur de l'Université de la Réunion doit être préalablement autorisée par le Président de l'Université ou son représentant.

Sont strictement prohibées les utilisations contraires aux lois et règlements en vigueur et notamment celles qui sont de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée des personnes.

4. Obligations des utilisateurs

4.1. Règles générales

- Les utilisateurs sont tenus de respecter la charte des bons usages de l'informatique de l'Université de la Réunion.
- Les utilisateurs doivent respecter les lois et règlements en vigueur ainsi que les règles de courtoisie et de politesse lors de l'utilisation des moyens informatiques de l'Université de la Réunion
- Les utilisateurs doivent faire une utilisation non-abusive des moyens informatiques auxquels ils ont accès.
- Les utilisateurs doivent respecter les mesures de sécurité des moyens informatiques prévues à l'article 6 de la présente charte.

4.2. Préservation des matériels et locaux.

- Les utilisateurs sont tenus de respecter les matériels, logiciels et locaux mis à leur disposition.
- Les utilisateurs qui constatent une dégradation ou un dysfonctionnement doivent, dans les plus brefs délais, informer le responsable de l'entité associée et le CRI.

4.3. Pénétration non autorisée dans les moyens informatiques.

- La pénétration non autorisée et le maintien dans un moyen informatique par un utilisateur sont interdits (art. 323-1 du Code Pénal).
- Les utilisateurs ne doivent pas utiliser ou tenter d'utiliser le compte d'un tiers. Est également interdite toute manœuvre qui viserait à accéder aux moyens informatiques sous une fausse identité ou en masquant l'identité véritable de l'utilisateur

4.4. Utilisation des comptes et des dispositifs de contrôle d'accès.

Les utilisateurs doivent prendre toutes les mesures nécessaires pour limiter les accès frauduleux aux moyens informatiques, et à ce titre ils doivent notamment :

- veiller à la confidentialité des codes, mots de passe, cartes magnétiques, clefs ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement personnel.
- veiller à la confidentialité des comptes utilisateurs qui leur sont attribués à titre strictement personnel.
- ne pas prêter, vendre ou céder les comptes utilisateurs, codes et autres dispositifs de contrôle d'accès ou en faire bénéficier un tiers.
- se déconnecter immédiatement après la fin de leur période de travail sur le réseau ou lorsqu'ils s'absentent.
- informer immédiatement le responsable de l'entité associé et le CRI de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect (art. 40 du Code de Procédure Pénal).
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles à des tiers.

- ne pas connecter un matériel sur le réseau de l'Université de la Réunion sans autorisation.
- ne pas utiliser de logiciels sans en avoir préalablement acquis la licence.

Le mot de passe d'un compte est une information personnelle qui ne doit être diffusé sous aucun prétexte, ni à un collègue, ni à un responsable (hiérarchique, informatique, ...). A travers cette information, un individu peut usurper une identité, déviant ainsi toute sanction vers le compte emprunté et non contre lui.

5. Charte éditoriale

Cet article s'impose à tout enseignant-chercheur, chercheur, administratif ou étudiant, membre de l'Université de la Réunion, souhaitant publier des informations ou des documents sur les sites de l'Université

L'usage du droit de publication devra respecter toute réglementation applicable dans ce domaine :

- respect des droits d'auteurs, du régime juridique des licences publiques et de la législation liés aux documents écrits et audiovisuels : chaque auteur devra s'assurer qu'il a le droit de diffuser les documents qu'il propose
- l'article L 122-5 du code de la propriété intellectuelle n'autorisant que les " copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective " et " les analyses et les courtes citations dans un but d'exemple et d'illustration ", toute représentation ou reproduction intégrale ou partielle faite sans consentement de l'auteur est interdite, les citations devront être courtes et leur source clairement indiquée
- respect du droit à l'image : il convient de vérifier que les images sont bien libres de droits ou d'obtenir une autorisation écrite du détenteur de ces droits
- conformément à l'article 34 de la loi " Informatique et Libertés " du 6 janvier 1978, les personnes citées disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent.

Le contenu des informations publiées sur les sites de l'Université doit respecter certaines règles :

- respect du service public
- pas de publicité commerciale. Les citations d'entreprises sont autorisées, si elles ne revêtent pas un caractère commercial
- s'interdire tout propos injurieux, diffamatoire, raciste, homophobe, sexiste, toute incitation à la haine raciale, toute attaque personnelle portant atteinte à la dignité d'une personne ou d'une fonction

6. Rôle du CRI

Les ressources informatiques de l'université sont administrées par le Centre de Ressources Informatiques (C.R.I.), qui s'engage à prendre toute disposition utile pour permettre le bon fonctionnement des ressources informatiques communes. De ce fait, il :

- autorise les accès aux moyens informatiques.
- attribue les comptes et les mots de passe ou tout autre dispositif permettant l'accès aux moyens informatiques conformément à la politique de l'établissement.
- assure le fonctionnement et la disponibilité normale des moyens informatiques.

Pour des nécessités de maintenance, de gestion technique, ou réglementaire, le CRI s'engage à :

- analyser et contrôler l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau (journalisation des échanges réseaux, journaux conservés trois mois conformément à la Loi sur la Sécurité Quotidienne du 31-10-2001 et art. 226-20 du Code Pénal), dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés
- surveiller en détail les sessions de travail d'un utilisateur soupçonné de non respect de la charte. Dans ce cas, il devra en informer le Président de l'Université et le Vice-Président du CEVU
- prendre les dispositions nécessaires à l'encontre d'un utilisateur ou d'un matériel informatique qui gênerait le bon fonctionnement des ressources informatiques.
- effacer ou compresser, les fichiers excessifs ou sans lien direct avec une utilisation normale du système informatique.

Les traitements automatisés de données nominatives mis en oeuvre par l'Université, ses composantes ou par tout utilisateur doivent respecter les dispositions de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

7. Modification et altération des moyens informatiques

En dehors des modifications ne portant pas atteinte au bon fonctionnement des moyens informatiques, aucune modification des environnements logiciels, matériels et périphériques ne pourra être effectuée sans l'accord préalable du responsable hiérarchique. Par modification d'environnement on entend toute suppression ou ajout de composants logiciels ou matériels ou tout paramétrage pouvant affecter le fonctionnement normal des moyens informatiques.

L'introduction, l'utilisation, la diffusion de tout dispositif logiciel ou matériel qui pourraient altérer les fonctionnalités des moyens informatiques sont interdites.

8. Conséquences des manquements à la charte et poursuites

8.1. Responsabilité des utilisateurs.

Chaque utilisateur est responsable de l'utilisation qu'il fait des moyens informatiques de l'Université de la Réunion ainsi que de l'ensemble des informations qu'il met à la disposition du public.

Chaque titulaire de comptes, ou d'un dispositif de contrôle d'accès, est responsable des opérations locales ou distantes effectuées depuis son compte ou sous le couvert des dispositifs de contrôle d'accès qui lui a été attribué.

Chaque utilisateur reconnaît que toute violation des dispositions de la présente charte ainsi que, plus généralement, tout dommage créé à l'université de la Réunion ou à des tiers engagera sa propre responsabilité.

8.2. Mesures applicables par les responsables informatiques

8.2.1. Mesures d'urgence

Le CRI peut en cas d'urgence :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques

8.2.2. Mesures donnant lieu à information

Sous réserve que soit informé le directeur ou le responsable du service, les responsables informatiques peuvent :

- avertir un utilisateur
- limiter provisoirement les accès d'un utilisateur
- à titre provisoire, retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes
- effacer, compresser ou isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril le fonctionnement des moyens informatiques
- informer le Responsable de la sécurité des Systèmes d'Information (RSSI)
- informer le Président de l'Université

8.2.3. Mesures soumises à autorisation du directeur ou responsable du service

Sous condition d'autorisation préalable du directeur ou du responsable de service, les responsables informatiques peuvent :

- retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes
- interdire à titre définitif à un utilisateur tout accès aux moyens informatiques dont il est responsable

8.3. Sanctions disciplinaires

Les utilisateurs ne respectant pas les règles et les obligations de la charte sont également passibles d'une procédure disciplinaire inhérente à leurs statuts. Ils peuvent être traduits devant la section disciplinaire du conseil d'administration de l'Université en ce qui concerne les étudiants et les enseignants-chercheurs et devant le conseil de discipline de leur corps respectif en ce qui concerne les personnels administratifs et techniques.

8.4. Poursuites civiles et pénales.

Tout utilisateur qui contreviendrait aux règles précédemment définies peut s'exposer à des poursuites civiles et/ou pénales prévues par les textes en vigueur (articles 323-1 à 323-7 du code pénal).