CHARTE D'UTILISATION DU SYSTEME D'INFORMATION DE L'ACADEMIE DE MARTINIQUE

Article 1 – Objet

Le bon fonctionnement du système d'information implique le respect des règles visant à assurer la sécurité, la performance des traitements, la préservation des données et le respect des dispositions légales et réglementaires qui s'imposent.
La présente charte, a pour objet de définir les règles, les prérogatives, les engagements et les responsabilités pour tout ce qui concerne le système d'information de l'Académie.
Elle a aussi pour vocation de sensibiliser les utilisateurs aux exigences de sécurité et d'attirer leur attention sur certains comportements pouvant porter atteinte à l'intérêt collectif du service public de l'éducation.

Article 2 – Définitions

Institution : tout service académique (rectorat, CIO, GIP, GRETA, circonscriptions, …) et tout établissement du premier et second degré.

Système d'information : ensemble des ressources permettant de collecter, regrouper, classifier, stocker, traiter et diffuser de l'information quel que soit le support (numérique, papier, …).
Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

Utilisateur : recouvre toute personne physique ayant accès aux ressources du système d'information quel que soit son statut et en particulier, les agents des services académiques. L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information. Il a une obligation de réserve et de discrétion à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[1].
En tout état de cause, les agents des services académiques sont soumis au respect des obligations résultant de leur statut ou de leur contrat.

Informatique nomade : ordinateurs portables, téléphones, smartphone, tablettes sont également un des éléments constitutifs du système d'information.

Ressource : élément informationnel, logiciel ou matériel.

DSI : désigne la Division des Systèmes d'Information du Rectorat. La DSI[2] a en charge l'administration et l'exploitation des systèmes ainsi que des infrastructures matérielles et logicielles.

[1] Notamment le secret médical et le secret professionnel pour les personnels de santé et sociaux.
[2] Contact DSI : dsi@ac-martinique.fr / Contact assistance informatique : assistance.informatique@ac-martinique.fr

Article 3 - Conditions d'utilisation des systèmes d'information

Utilisation professionnelle / privée

Les systèmes d'information sont des outils de travail ouverts à des usages professionnels administratifs et pédagogiques. Ils peuvent également constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle du matériel informatique, des outils de communication et des espaces de stockage à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévues explicitement[3] à cet effet ou en mentionnant le caractère privé sur la ressource[4]. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou des services académiques, il lui appartient de détruire cet espace, la responsabilité de l'administration ne pouvant être engagée quant à sa conservation.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur.

En particulier, la détention, diffusion et exportation d'images à caractère pédophile[5], ou la diffusion de contenus à caractère raciste ou antisémite[6] est totalement interdite.

De même, la consultation de sites à caractère pornographique depuis les réseaux des services académiques est interdite.

Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition.

Article 4 - Principes de sécurité

Règles de sécurité applicables

Le Rectorat met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

[3] Pour exemple, cet espace pourrait être dénommé "_privé_"
[4] Pour exemple, "_privé_nom_de_l_objet_» : l'objet pouvant être un message, un fichier ou toute autre ressource numérique.
[5] Article 327-23 du Code pénal
[6] Article 24 24 bis de la Loi du 29 juillet 1881

Les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- de garder strictement confidentiel son (ou ses) code d'accès et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

- de la part de l'institution :
  - veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées ;
  - limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- de la part de l'utilisateur :
  - s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
  - ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'institution, ou ceux validés par la DSI ;
  - ne pas installer, télécharger ou utiliser sur le matériel de l'institution, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de la DSI ;
  - se conformer aux dispositifs mis en place par la DSI[7] pour lutter contre les virus et les attaques par programmes informatiques.

Devoirs de signalement et d'information

L'utilisateur doit avertir le Responsable Sécurité des Systèmes d'Information (rssi@ac-martinique.fr) dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information. Il informe également sa hiérarchie.

Il signale à la DSI toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

L'utilisateur doit informer sa hiérarchie qu'il est détenteur d'un dispositif d'authentification forte (type clé OTP[8]) remis par l'institution et de tout dispositif lui permettant d'accéder à distance au réseau intranet des services académiques.

[7] Contact direction DSI : dsi@ac-martinique.fr / Contact plateforme d'assistance : assistance.informatique@ac-martinique.fr ou 05 96 52 25 25

[8] OTP : One Time Password (mot de passe utilisable une fois) offrant une authentification forte à l'utilisateur.

Mesures de contrôle de la sécurité

L'institution se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à la disposition de l'utilisateur.

Elle l'informe :

- des maintenances correctives, curatives ou évolutives ;
- des maintenances à distance ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire sera isolée ; le cas échéant supprimée.

Le système d'information peut donner lieu à une surveillance et à un contrôle à des fins statistiques de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels de la DSI chargés des opérations de l'administration et du contrôle des systèmes d'information sont soumis à obligation de discrétion. Ainsi, ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur. En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'alinéa 2 de l'article[9] 40 du code de procédure pénale.

Article 5 - Communication électronique – Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein des services académiques.

Adresses électroniques

Le Rectorat s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative[10] lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins des services académiques.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'« utilisateurs», relève de la responsabilité exclusive du Rectorat : ces listes ne peuvent être utilisées sans autorisation explicite de l'autorité académique.

[9] Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.
[10] Par exemple, l'adresse est de la forme prénom.nom@ac-martinique.fr

Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[11] ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par la DSI.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques…).

Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

L'utilisateur doit limiter l'usage des fichiers joints de gros volume, particulièrement lorsqu'il s'agit de diffusion en masse. Il privilégiera d'autres outils mis à disposition par la DSI pour de tels besoins (espace collaboratif, service de partage de fichiers…).

Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles[12] 1125 à 1127-4 du Code civil.

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve. Les équipes d'assistance de la DSI apportent l'accompagnement technique nécessaire.

En cas d'absence prolongée et de mutation de l'utilisateur

L'utilisateur doit utiliser le gestionnaire d'absence de l'outil de messagerie qui permet de renseigner le texte de la réponse automatiquement adressée en un seul envoi à chaque expéditeur. Il précisera la période d'absence et les coordonnées du secrétariat de son service et des éventuelles collaborateurs à contacter en cas de nécessité.
Dans le cas d'une mutation ou d'un départ à la retraite la boite aux lettres nominative de l'agent est conservée pendant une durée de 9 mois.
En cas de mutation pour une autre académie, la boite électronique nominative de l'utilisateur sera nécessairement close et une nouvelle devra être créée dans l'académie d'accueil.

[11] Pour exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message
[12] Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne

Afin de garantir la continuité de service tout utilisateur concerné par une absence prolongée doit communiquer avant son départ à son supérieure hiérarchique toutes les informations professionnelles nécessaires pour la poursuite des traitements des dossiers dont il avait la charge. En revanche, la récupération des informations personnelles présentent dans sa boite électronique académique sont à la charge de l'agent.

Limitation de l'utilisation du protocole imaps et pops

La messagerie académique permet d'utiliser des logiciels de messagerie sur les terminaux (PC, portables, tablettes, smartphones,). Les protocoles d'échanges et de synchronisation sécurisés imaps et pops sont pour cela disponibles. Il est cependant interdit de les intégrer sur une plateforme ou un environnement de travail privé et non explicitement autorisé par la DSI. Par exemple, il est interdit d'utiliser les fonctionnalités d'intégration de votre boite académique sur des sites comme Gmail ou Yahoo mail…

Article 6 – Réseaux Internet et Intranet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques). Si une utilisation résiduelle privée, telle que définie à l'article 3 « Utilisation professionnelle / privée », peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'institution sont présumées avoir un caractère professionnel. L'institution peut les rechercher aux fins de les identifier.

Publication sur les sites web de l'institution

Toute publication de pages d'information sur les sites internet ou intranet académiques doit être validée par le responsable de site ou responsable de publication nommément désigné.

Sécurité

Le Rectorat se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

Ce contrôle est autorisé au travers des dispositifs de sécurité mis en place par l'institution.

Conditions d'utilisation des réseaux

Le Rectorat étant connecté à l'internet via RENATER « Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche », les utilisateurs doivent respecter la charte déontologique RENATER disponible ici :
https://www.renater.fr/fr/telechargement%2C1392

Les conditions d'utilisation des systèmes d'information et les principes de sécurité précisés dans les paragraphes précédents s'appliquent à l'utilisation des réseaux. Il est en outre précisé les règles suivantes :

- ne pas récolter ou collecter d'informations concernant des tiers sans leur consentement ;
- ne pas diffamer, diffuser, harceler, traquer, menacer quiconque, ni violer les droits d'autrui ;
- ne pas créer une fausse identité ;

- ne pas adresser de message indésirable à caractère malveillant communément appelé spam ;
- ne pas adresser de message électronique comprenant des propos injurieux, diffamatoires, obscènes, indécents, illicites ou portant atteinte à tout droit, notamment les droits de la personne humaine et la protection des mineurs ;
- ne pas transmettre de virus, cheval de Troie, bombe logique ou tout autre programme nuisible ou destructeur pour des tiers. À cet égard, il appartient à l'utilisateur de vérifier qu'il dispose des équipements matériels, logiciels (antivirus à jour…), navigateurs lui permettant d'utiliser le service internet ;
- ne pas perturber les services, données et/ou contenus auxquels il accède ;
- ne pas envoyer des chaînes de lettres ou proposer des ventes dites « boule de neige » ou « pyramidale » ;
- ne pas envoyer de publicité, de message promotionnel ou toute autre forme de sollicitation non désirée à d'autres utilisateurs ;
- ne pas utiliser sur le réseau du Rectorat des moyens de cryptologie qui n'auraient pas fait l'objet des déclarations ou des autorisations imposées par **les articles 29 à 33 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;**
- ne pas fournir d'accès indirect au réseau RENATER.

La connexion aux réseaux de l'Institution peut demander une authentification. Elle s'effectue à l'aide du compte académique (identifiant et mot de passe personnel qu'il convient de changer régulièrement°. Dans certains cas une authentification forte par clé de sécurité « OTP[13] » est nécessaire.

Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle.

Le Rectorat se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution, codes malveillants, programmes-espions…).

Article 7 – Traçabilité

Le Rectorat est dans l'obligation légale de mettre en place un système de journalisation[14] des accès Internet, de la messagerie et des données échangées. Pour cela, des outils de traçabilité sur tous les systèmes d'information ont été mis en place.

Des fichiers de « traces » peuvent être générés par les systèmes. Ils correspondent à un historique des actions effectuées par les utilisateurs. Ils peuvent être utilisés pour un usage technique et servir à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés.

Le Rectorat s'engage à ne pas transmettre ces données de traçabilité, à ne pas divulguer les informations de connexions collectées et à respecter les correspondances privées reçues ou transmises par l'utilisateur sur le réseau Internet.

[13] OTP : One Time Password (mot de passe utilisable une fois) offrant une authentification forte à l'utilisateur.
[14] Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur

Il peut être fait exception à cette règle de confidentialité dans les limites autorisées par la loi, à la demande des autorités publiques et/ou judiciaires ou pour toute recherche sur des flux ne respectant pas la présente charte.

De plus, depuis le décret du 2 mars 2006, relatif à la conservation des données des communications électroniques, ces « traces » doivent être conservées pendant un an. Seuls les en-têtes de mails sont conservés. Dans le cadre d'une procédure judiciaire, ces fichiers doivent pouvoir être mis à la disposition de la justice « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ».

Article 8 - Respect de la propriété intellectuelle

L'utilisation des ressources informatiques implique le respect des droits de la propriété intellectuelle.

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Article 9 – Traitement des données à caractère personnel

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Il est rappelé la nécessité de respecter les dispositions légales en matière de traitement des données à caractère personnel, notamment conformément à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée et du RGPD (Règlement Général de la Protection des Données).

En conséquence, tout utilisateur souhaitant procéder à un traitement de données à caractère personnel doit obtenir l'autorisation du responsable des traitements afin d'inscrire ce traitement dans le registre dédié. Il convient de s'adresser au Délégué à la Protection des Données à l'adresse (dpd@ac-martinique.fr)

Par ailleurs, chaque utilisateur dispose d'un droit d'accès et de rectification et d'effacement relatif à l'ensemble des données le concernant dans le respect de la réglementation, y compris les données portant sur l'utilisation des systèmes d'Information.

L'utilisateur peut demander l'effacement de ses données personnelles dans les cas prévus à l'article 17 du RGPD.

Un droit à la portabilité des données personnelles est instauré par le RGPD. L'utilisateur peut à tout moment demander à recevoir ou transférer ses données personnelles à un autre responsable des traitements lorsque cela est techniquement possible. Le format de ces données doit être structuré et lisible par machine.

Un délégué à la protection des données est désigné par le Recteur de l'académie.

Ses principales missions sont de contrôler le respect du RGPD, de conseiller le responsable des traitements, de faire office de point de contact avec l'autorité de contrôle et le DPD national, de répondre aux sollicitations des usagers qui souhaitent exercer leurs droits.

Le délégué à la protection des données de l'Académie de la Martinique est joignable à l'adresse dédiée suivante : dpd@ac-martinique.fr

Article 10 - Limitation des usages

En cas de non-respect des règles définies dans la présente charte, la «personne juridiquement responsable»15 pourra, sans préjuger des procédures judiciaires et administratives pouvant être engagées à l'encontre de l'utilisateur, restreindre par mesure conservatoire ses usages aux SI. Tout abus dans l'utilisation des ressources à des fins extra-professionnelles par l'utilisateur est passible de sanctions.

ARTICLE 11 – Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entrainer à son encontre des avertissements, des limitations ou suspension d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

ARTICLE 12 –Diffusion de de la Charte

La présente charte est communiquée individuellement à chaque agent.
La présente charte est disponible sur l'intranet de l'Académie.
Des opérations de communication interne sont organisées de manière régulière, afin d'informer les agents sur les pratiques d'utilisation des services numériques recommandées.
Par ailleurs, chaque agent doit assurer régulièrement une veille informationnelle sur les bonnes pratiques de sécurité diffusées par les instances gouvernementales

La présente charte est applicable à compter du 1er Février 2020
Elle a été adoptée après information du Comité Technique Académique du 28 janvier 2020.

[15] Personne juridiquement responsable (PJR) : le Recteur de l'académie de la Martinique