Règlement intérieur de l'Université de Reims Champagne-Ardenne

SOMMAIRE

Annexe 1 : Règlement intérieur « hygiène, sécurité, santé, environnement » de l'URCA
Annexe 2 : Charte de sécurité de l'administrateur informatique au sein de l'université de Reims Champagne-Ardenne
Annexe 3 : Charte régissant l'usage du système d'information au sein de l'université de Reims Champagne-Ardenne
Annexe 4 : Politique de sécurité des systèmes d'information (PSSI) Université de Reims Champagne Ardenne

Préambule :

Le règlement intérieur de l'Université de Reims Champagne-Ardenne est édicté en application de l'article L712-3 du code de l'éducation, donnant compétence au conseil d'administration de l'Université pour adopter le règlement intérieur de l'université. Il a pour objet de compléter les règles institutionnelles prévues par les statuts, qu'il ne saurait modifier, pour assurer le fonctionnement intérieur de l'Université. Il recense les règles internes prises dans le cadre des activités de l'Université et qui sont opposables aux étudiants et personnels. Ce règlement a vocation à s'appliquer à l'ensemble des membres de la communauté universitaire, usagers et personnels, ainsi qu'à toute personne physique ou morale présente, à quelque titre que ce soit, au sein de l'URCA.
Il peut être complété par des mesures d'ordre interne, délibérations, décisions, arrêtés.

Il arrête les conditions d'application des statuts, et notamment celles concernant :

- l'organisation de l'Université ;
- les droits et obligations ;
- l'hygiène et la sécurité dans les locaux et enceintes universitaires ;
- l'ordre dans les enceintes et locaux universitaires ;
- les moyens de communication et la charte informatique.

Conformément au Code de l'Education et aux dispositions de l'article 4 des statuts, l'Université comprend des composantes d'enseignement et de recherche, que sont les Unités de Formation et de Recherche et les Instituts, des services communs et des services généraux, et des services centraux.
Les UFR, instituts, services communs et services généraux sont dirigés par des personnels élus ou nommés par le président ou le Ministre conformément aux statuts de ces composantes.
Le directeur général des services assure, sous l'autorité du président de l'université, la direction, l'organisation et le fonctionnement des services administratifs, financiers et techniques de l'établissement.

Le présent règlement intérieur fait l'objet d'une publication, par voie d'affichage, dans tous les locaux universitaires et sur le portail numérique de l'Université (intranet).

TITRE I : DE L'ORGANISATION DE L'UNIVERSITE

SOUS-TITRE 1 : DISPOSITIONS COMMUNES AUX CONSEILS CENTRAUX

Article 1: Fonctionnement des conseils centraux

Les présentes dispositions sont communes aux conseils centraux de l'université : le conseil d'administration, le conseil académique et ses deux commissions : la commission de la formation et de la vie universitaire et la commission recherche.

Les conseils centraux et commissions sont présidés par le président de l'université ou en cas d'empêchement par les Vice-présidents désignés à cet effet. Il est établi un ordre du jour des séances.

Cet ordre du jour est préparé par le président, assisté du Vice-président concerné, et adressé aux membres de ce conseil au moins 8 jours avant la date du conseil. Les documents préparatoires sont envoyés en même temps que l'ordre du jour, sauf circonstances

exceptionnelles. Toute modification de l'ordre du jour, est soumise à l'approbation du conseil en début de séance.

Au début de chaque séance, il est procédé à l'approbation du procès-verbal de la séance précédente. Le président de séance vérifie la présence des conseillers, soit par un appel nominal, soit par la mise en circulation d'une feuille d'émargement, et donne lecture des pouvoirs.
Le président assure la police de la séance et dirige les débats. Il lui appartient d'ouvrir et de lever la séance. Il peut déterminer un temps limité de paroles pour un point à l'ordre du jour. Lorsqu'un point à l'ordre du jour appelle à être débattu, le président organise les demandes de prises de paroles, à tour de rôle.

Lorsqu'au moins deux orateurs d'avis contraires ont pris part à une discussion sur un point de l'ordre du jour et traité le fond du débat, le président de séance peut proposer la clôture de la discussion. Un seul membre du Conseil peut alors être entendu contre la clôture et doit se limiter à cet objet. Le président de séance met ensuite la clôture aux voix. Lorsque la clôture a été adoptée, seuls les orateurs déjà inscrits dans le débat peuvent intervenir.

Le secrétariat des réunions du conseil d'administration, en particulier le registre des présences et procurations, est assuré par l'administration de l'URCA.

Les votes ordinaires ont lieu, en principe, à main levée. Ils se font à bulletin secret sur demande d'un quart des membres présents ou représentés. En outre, les votes se font à bulletin secret pour les questions à caractère nominatif et celles relatives aux élections, désignations et propositions concernant des personnes nommément désignées.

Une suspension de séance peut être décidée par le président ou à la demande du tiers des membres présents ou représentés.

La procuration prévue par les statuts (*les membres ne peuvent détenir plus de deux procurations*) peut être accordée par un membre du conseil à n'importe quel autre membre du même conseil, sauf pour les représentants des collectivités et organismes dont la suppléance est prévue.

La procuration doit être nominale et ne peut être transmise. En ce qui concerne les conseils restreints, tout conseiller ne peut représenter qu'un conseiller de son propre collège.

Le texte d'un amendement est toujours mis aux voix avant le texte qu'il amende

Afin de garantir la confidentialité des débats, seuls les tiers invités à être entendus peuvent être destinataires des messages envoyés par les membres du conseil dans le cadre de la délibération qui les concernent directement.

Article 2 : Relevé de décisions

Un relevé de décisions est élaboré suivant le conseil, dans les plus brefs délais. Ce relevé de décisions reprend le sommaire de l'ordre du jour, et mentionne le vote du conseil. Il est transmis au Président pour approbation, et diffusé largement par le cabinet de la présidence. Ce relevé est consultable sur le site intranet de l'Université.

Article 3 : Dispositions relatives aux modalités de publicité du budget de l'université

Le budget est rendu public au plus tard un mois après avoir été, selon le cas, adopté, arrêté ou approuvé. Dans le mois qui suit l'adoption du budget de l'université, celui-ci est rendu public au cours de l'année civile de référence. Il sera mis à disposition au sein des locaux de la Direction

des Affaires financières de l'université de Reims Champagne-Ardenne. Il sera affiché, dans sa version numérique, sur l'intranet de l'université.

SOUS-TITRE 2 : LES COMMISSIONS

Article 4 : Dispositions générales

Des commissions peuvent être constituées à l'initiative du conseil d'administration ou sur proposition du président. Des groupes de travail peuvent être constitués à l'initiative des commissions du conseil Académique ou sur proposition du président. Le président de l'université est membre de droit des commissions et groupes de travail.

La durée du mandat des membres des commissions est de quatre (4) ans sauf pour les représentants étudiants dont le mandat est de deux (2) ans, elles sont renouvelées après l'élection des membres du conseil d'administration. Le mandat des membres des commissions prend fin à l'occasion du renouvellement des représentants des membres des conseils.

En cas d'absence non justifiée d'un membre à 3 réunions consécutives, le président de l'université propose au conseil d'administration son remplacement. Tout siège devenu vacant donne immédiatement lieu à un renouvellement, pour la durée du mandat restant à courir.

Les conseils centraux, autres conseils ainsi que les commissions peuvent se réunir à distance ou être consultés par échanges d'écrits par voie électronique et ce, conformément au décret n°2014-627 du 26 décembre 2014 relatif aux modalités d'organisation des délibérations à distance des instances administratives à caractère collégial et à l'ordonnance n°2014-1329 du 6 novembre 2014 relative aux délibérations à distance des instances administratives à caractère collégial.

En cas de réunion à distance, les échanges en visioconférence ou en audioconférence ne sont pas enregistrés. Les échanges par messagerie instantanée sont supprimés dans les quinze jours suivant la séance.
Si le conseil se réunit pour une question relevant d'une certaine technicité, sous réserve de l'approbation par au moins la majorité des membres participants, le président pourra demander l'enregistrement des échanges. Ceux-ci ne seront utilisés que pour la rédaction des PV/comptes rendus… et seront supprimés dès approbation des documents lors de la réunion suivante du conseil.

La participation de tiers aux réunions à distance des conseils de l'établissement est régie dans les conditions prévues par les règles internes de chaque instance pour les réunions en présentiel. La participation des services administratifs ou techniques, afin de permettre notamment le bon déroulement de la séance ou la prise de note en vue de la rédaction des comptes-rendus/PV…, s'inscrit dans le parallèle des conditions des séances en présentiel.

Article 5 : La commission des statuts

Mission

Elle est chargée, sous la présidence du président de l'université ou du représentant institutionnel désigné à cet effet, de préparer les délibérations du conseil d'administration relatives aux statuts de l'université. Elle est notamment consultée sur tout projet de modification des statuts de l'université, des composantes ou services communs et généraux. Elle propose également la constitution du règlement intérieur de l'université prévu dans les statuts et en examine les demandes de modifications. Les avis de la commission des statuts sont transmis au conseil d'administration.
Les membres de la commission des statuts sont élus par le conseil d'administration de l'université.

Le Directeur général des services est membre consultatif de la commission des statuts.

Composition

La commission des statuts est élue au scrutin plurinominal majoritaire à deux tours par le conseil d'administration, et comprend douze membres :

- le représentant institutionnel désigné à cet effet ;
- 6 enseignants (3 du 1er collège, 3 du 2ème collège) ;
- 3 étudiants ;
- 2 représentants des BIATSS.

Article 6 : La commission des moyens

Mission

Elle est chargée, sous la présidence du président de l'université ou du représentant institutionnel désigné à cet effet, de préparer les délibérations du conseil d'administration relatives au budget de l'université. Elle peut être consultée sur les modalités de fixation de rémunérations et de tarifs. Elle donne un avis sur l'acceptation de dons et legs, et en général, sur tous projets comportant un aspect financier. Elle analyse tous les documents budgétaires de l'établissement.

Composition

La commission des moyens, est élue au scrutin plurinominal majoritaire à deux tours par le conseil d'administration, et comprend douze membres :

le représentant institutionnel désigné à cet effet ;
6 enseignants (3 du 1er collège, 3 du 2ème collège) ;
3 étudiants ;
2 représentants des BIATSS.

Article 7 : La Commission Pour les Relations Internationales (CPRI)

Mission

Elle est chargée, sous la présidence du président de l'université ou du représentant institutionnel désigné à cet effet d'émettre des propositions pour la mise en place de procédures dans le cadre de la démarche qualité conformes aux exigences prévues par les textes et organise la mise en œuvre de la mobilité internationale entrante et sortante des étudiants et des personnels dans le cadre de programmes institutionnels en pédagogie et en recherche.

Elle procède à :

- un point d'information sur l'action internationale de l'établissement ;
- la définition des critères d'attribution des aides à la mobilité internationale pour les mensualités supplémentaires ;
- la définition des appels à projet des dispositifs de soutien à la mobilité internationale
- l'examen des programmes d'échanges extracommunautaires ;
- l'examen des projets internationaux susceptibles d'obtenir un cofinancement de l'université;
- l'examen des projets de diplôme en partenariat international ;

- l'examen des candidatures aux dispositifs de soutien à la mobilité internationale.

Composition

La Commission Pour les Relations Internationales « CPRI » est présidée par le représentant institutionnel délégué aux Relations internationales. Elle est composée des membres suivants :

- le représentant institutionnel délégué aux relations internationales ;
- le vice-président étudiant ;
- un représentant de chaque école doctorale
- un représentant par composante élu par le conseil de la composante ;
- 2 enseignants, chercheurs ou enseignants-chercheurs, élus de la Commission de la Formation et de la Vie universitaire (CFVU) tels que définis par l'article L719-1 du Code de l'Éducation ;
- 2 étudiants élus de la CFVU tels que définis par l'article L719-1 du Code de l'Éducation ;
- 1 représentant BIATSS élu de la CFVU ;
- 2 chercheurs ou enseignant-chercheurs élus de la Commission Recherche (CR) tels que définis par l'article L719-1 du Code de l'Éducation ;
- 2 étudiants élus de la CR tels que définis par l'article L719-1 du Code de l'Éducation ;
- 1 représentant BIATSS élu de la CR
- 1 représentant élu du CA ;

Les EPCI auxquels se rattachent les villes de Reims et Troyes, la Région Grand-Est, le CROUS, les responsables de la direction des Relations Extérieures et du Développement International (DREDI), de la direction des Études et de la Vie étudiante (DEVU), de la direction de la Recherche et de la Valorisation, de la Maison des Langues, les Vice-Présidents et chargés de mission de l'URCA dont les missions entrent dans le champ de compétence de la CPRI, et les directeurs de développement sont invités permanents de la CPRI.

La Commission Pour les Relations Internationales présente un bilan annuel de ses activités qu'elle transmet aux conseils de l'établissement.

La CPRI siègera en commission plénière ou restreinte aux membres élus au moins deux fois par an.

Article 8 : Commission sociale plénière

Il est institué, au sein de l'URCA, une commission sociale plénière en faveur des personnels. La commission sociale plénière se réunit deux fois par an.

Mission

La commission sociale plénière a pour rôle :
- de proposer au président les orientations de l'action sociale de l'URCA ;
- de mettre en œuvre les mesures destinées à développer l'action sociale de l'URCA ;
- d'analyser le bilan de l'action sociale établi par le service d'action sociale.

Composition :

La composition de la commission sociale en faveur des personnels est fixée comme suit :

Au titre de l'administration :

- Le président de l'Université ou le représentant qu'il désigne ;

- Le Directeur général des services ;
- Le Directeur des ressources humaines ;
- Le Directeur des affaires financières ;
- Le responsable du service d'action sociale ;
- Le président du Comité d'Action sociale de l'université (CASUR) ;
- Un expert.

Au titre des représentants de chaque organisation syndicale :

- 1 représentant titulaire et suppléant de chaque organisation syndicale représentée au Comité Technique.

Le service d'action sociale participe aux réunions de la commission sociale plénière afin d'apporter à cette instance les éléments d'information dont il dispose sur les besoins des agents de l'URCA. Le président de la commission peut solliciter la présence d'experts et invités. Ils sont convoqués par le président quarante-huit heures au moins avant le début de la réunion.

Article 9 : Le conseil de perfectionnement de l'organisme de formation par apprentissage

La présidence du conseil de perfectionnement est assurée par le président de l'université et par délégation son représentant.
Le conseil de perfectionnement est organisé, au minimum, une fois par an.

Attributions :
Le conseil de perfectionnement examine et débat des questions relatives à l'organisation et au fonctionnement du centre de formation d'apprentis, notamment sur :

1. Le projet pédagogique du centre de formation d'apprentis ;
2. Les conditions générales d'accueil, d'accompagnement des apprentis, notamment des apprentis en situation de handicap, de promotion de la mixité et de la mobilité nationale et internationale ;
3. L'organisation et le déroulement des formations ;
4. Les conditions générales de préparation et de perfectionnement pédagogique des formateurs ;
5. L'organisation des relations entre les entreprises accueillant des apprentis et le centre ;
6. Les projets de convention à conclure, en application des articles L. 6232-1 et L. 6233-1, avec des établissements d'enseignement, des organismes de formation ou des entreprises ;
7. Les projets d'investissement ;
8. Les informations publiées chaque année en application de l'article L. 6111-8.

Composition :
Le conseil de perfectionnement comprend 9 membres :

- Le président de l'URCA ou son représentant ;
- Le directeur de la formation continue et de l'alternance ;
- 1 représentant des organisations professionnelles d'employeurs,
- 1 représentant des organisations professionnelles de salariés
- 3 représentants des personnels d'enseignement intervenant pédagogiquement ou administrativement dans les formations en apprentissage gérées par l'URCA au titre de son OFA.
- 2 représentants élus des apprentis de l'URCA en cours de formation au titre de son OFA.

Les organisations professionnelles d'employeurs et de salariés siègeront à tour de rôle tous les 2 ans, l'ordre étant déterminé par tirage au sort lors de la première réunion du conseil.

Les représentants des personnels d'enseignement sont désignés par le président de l'université pour une durée de 4 ans

Les représentants des apprentis sont élus pour un mandat d'un an au scrutin uninominal majoritaire à un tour.

Le conseil de perfectionnement délibère valablement lorsque la majorité de ses membres en exercice sont présents ou représentés. Lorsqu'à l'issue de la première réunion, ce quorum n'a pas été atteint, une seconde réunion, avec le même ordre du jour, se tient sans condition de quorum dans un délai de 8 jours.

Chaque membre peut donner procuration à un autre membre. Nul ne peut être porteur de plus de deux procurations. Les avis du conseil de perfectionnement sont pris à main levée, à la majorité simple.

Le conseil de perfectionnement peut inviter toute personne qu'il juge utile de consulter.

Titre II : DROITS ET OBLIGATIONS

Article 10 : Liberté de réunion, d'association, d'affichage, de publication et de représentation :

Article 10.1 liberté de réunion :

Elle s'exerce en conformité avec l'article L811-1 du code de l'éducation concernant la liberté d'expression et d'information à l'égard des problèmes politiques, économiques, sociaux et culturels. Des locaux sont mis à la disposition.
Les demandes doivent être déposées à l'avance auprès des services administratifs et accordées par le responsable de site.

Ces réunions doivent respecter les programmes des activités d'enseignement et de recherche et se dérouler en toute sécurité en respectant l'intégrité des matériels et des locaux. Elles ne peuvent avoir un objet commercial ou publicitaire et doivent respecter le principe de laïcité.

Article 10.2 liberté d'association : associations étudiantes et syndicats étudiants.

Elle s'exerce dans les conditions de l'article L811-3 du code de l'éducation. Les différentes organisations étudiantes doivent avoir pour objet la défense des droits et des intérêts matériels et moraux, tant collectifs qu'individuels des étudiants. Elles doivent respecter les règles de laïcité et de neutralité et rester compatibles avec les principes du service public d'enseignement. Les membres de ces organisations doivent avoir un lien étroit avec l'université et réunir des étudiants appartenant majoritairement à l'université.

Toute association étudiante souhaitant bénéficier des services de l'université doit signer la convention des associations étudiantes de l'URCA. Toute association étudiante pourra solliciter la mise à disposition temporaire de locaux dans la limite des disponibilités et des priorités de l'université. La mise à disposition d'un local est subordonnée à la signature par les associations concernées d'une convention d'occupation précaire du domaine public de l'université. Les conditions de réservation sont propres à chaque structure dans le respect des dispositions générales en vigueur à l'Université.

La CFVU (Commission de la Formation et de la vie universitaire) est la garante des libertés politiques et syndicales des étudiants.

Article 10.3 liberté syndicale :

Le Président de l'université est le garant du libre exercice des libertés syndicales des personnels et des usagers dans le cadre des dispositions législatives et réglementaires. Les organisations syndicales représentatives des personnels disposent de locaux au sein de l'université et de moyens nécessaires à l'exercice de leurs activités. Elles disposent également de panneaux d'affichage réservés à cet effet.

Article 10.4 Affichage et diffusion des informations syndicales :

L'affichage est autorisé, dans les conditions prévues par le décret n°82-447 du 28 mai 1982 sur des panneaux prévus à cet effet et mis à la disposition des étudiants et des personnels mais reste interdit dans les parties communes (murs, couloirs, …). Cet affichage ne peut être anonyme ni porter atteinte à l'honneur, au droit d'autrui ou à l'ordre public. Il ne peut donner lieu à des actes de propagande ni de prosélytisme.

L'affichage dans les composantes et les locaux de recherche est placé sous la responsabilité de leurs directeurs respectifs.

Des listes de diffusion sont mises à disposition des organisations syndicales représentatives des personnels.

Article 10.5 Droit de publication :

Les publications rédigées par les étudiants peuvent être diffusées librement mais ne doivent être ni anonymes, ni présenter un caractère injurieux, diffamatoire ou discriminatoire et ne peuvent porter atteinte à l'ordre public ni aux droits d'autrui conformément aux lois qui s'appliquent à la presse. En cas de diffusion de publications contraires au règlement, la responsabilité des auteurs est pleinement engagée devant les tribunaux compétents. La distribution de documents non pédagogiques ne peut se faire qu'en dehors des activités pédagogiques (cours, T.D, T.P).

Article 10.6 Droit de représentation :

Conformément au Code de l'Education, les usagers sont électeurs et éligibles et sont représentés dans les conseils et commissions de l'Université ainsi que sur proposition du Président dans le bureau qui assiste le Président. La présence dans les différentes instances justifie l'absence à des cours, des T.D et des T.P.

Article 11: Activités commerciales

Tout commerce ou vente est interdit, les activités et la publicité commerciale sont interdites conformément aux articles L442-11 du code de commerce et 446-1 du code pénal excepté lorsqu'une convention ou une autorisation spécifique a été délivrée par le Président de l'Université ou son représentant.

Article 12 : Comportement

Le comportement des personnes (usagers, personnels de l'université, toute autre personne présente au sein de l'université à quelque titre que ce soit) doit être conforme aux règles communément admises en matière de vie en société, de respect d'autrui, de civilité, de respect des bonnes mœurs ainsi qu'aux lois et règlements en vigueur.
Les actes, écrits, attitudes ou propos ne doivent pas porter atteinte à l'ordre public et au bon fonctionnement de l'université.
Ils ne doivent pas créer une perturbation dans le déroulement des activités d'enseignement, de

recherche, administrative, culturelle et sportive et de toute manifestation autorisée dans les enceintes et locaux universitaires.
Ils ne doivent pas non plus porter atteinte à la santé, l'hygiène et la sécurité des personnes et des biens.
Tout personnel ou tout usager qui proférerait des menaces et exercerait des violences verbales ou physiques à l'égard d'autrui sera poursuivi devant la section disciplinaire compétente, indépendamment de la mise en œuvre de poursuites pénales à raison des mêmes faits. Les sanctions disciplinaires encourues peuvent aller jusqu'à la révocation, pour les personnels, à l'exclusion définitive.

Article 13 : Actes discriminants

Aux termes des dispositions législatives en vigueur, tout acte raciste, antisémite, xénophobe, homophobe, sexiste ou discriminant est passible de poursuites pénales. De même, toute discrimination fondée sur l'appartenance ou la non-appartenance, vraie ou supposée, à une ethnie ou une race, sa religion, ses convictions, son âge, son handicap, son orientation ou identité sexuelle, son sexe ou son lieu de résidence, est interdite. Cette législation s'applique aux personnels et aux usagers de l'université. Toute infraction dûment constatée à ces dispositions, qu'il s'agisse d'agressions physiques, d'écrits ou de propos inconvenants, fera l'objet de procédures disciplinaires dans le cadre réglementaire. Les sanctions disciplinaires encourues peuvent aller jusqu'à la révocation, pour les personnels, à l'exclusion définitive de tout établissement public d'enseignement supérieur, pour les usagers. En outre, l'université se réserve le droit d'engager devant les tribunaux les procédures pénales qui s'imposent contre les personnes responsables de tels agissements au sein de la communauté universitaire.

SOUS-TITRE 1 : DISPOSITIONS APPLICABLES AUX USAGERS

Article 14 : Harcèlement

L'université, lieu de formation et de recherche, se doit de respecter et de faire respecter les droits de ses personnels et de ses usagers et de s'assurer que les relations professionnelles et pédagogiques se déroulent dans le respect et la dignité de chacun.
Toute forme de harcèlement est interdite et soumise à des sanctions.
Le harcèlement moral consiste dans le fait de harceler autrui par des agissements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptibles de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel (Article 222-33-2 du code pénal)
Le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou des comportements à connotation sexuelle qui soit, portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante.
Est assimilé au harcèlement sexuel le fait, même non répété, d'user de toute forme de pression grave dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur ou au profit d'un tiers. (Article 222-33 du Code pénal)

Indépendamment de la mise en œuvre de poursuites pénales, des poursuites disciplinaires peuvent être engagées à l'égard des auteurs des faits. En outre, toute personne, s'il est avéré qu'elle a, par son comportement, organisé, encouragé, facilité le harcèlement ou si elle s'est abstenue de toute intervention pour l'empêcher peut également faire l'objet de poursuites disciplinaires.

Toute personne qui estime être victime d'une forme de harcèlement peut en faire état auprès du SUMPPS pour les usagers ou du médecin de prévention pour les personnels.
Toute personne témoin d'une situation de harcèlement doit en faire le signalement au Président

de l'université.

Le CHSCT doit être tenu informé de toutes les situations de harcèlement et peut proposer des moyens d'y remédier.

Article 15 : Mesures sanitaires exceptionnelles

Tout personnel ou tout usager ne respectant pas les mesures sanitaires, notamment le port du masque et les gestes barrières, lorsqu'elles sont rendues obligatoires par les autorités compétentes commet une faute susceptible de poursuites disciplinaires sans préjudice de l'éviction immédiate de la personne concernée.

Article 16 : Notion d'usager

Sont usagers de l'université les bénéficiaires des services d'enseignement en formation initiale ou continue, de recherche et de diffusion des connaissances, en application du code de l'éducation.
Les usagers de l'université comprennent les étudiants inscrits en vue de la préparation d'un diplôme ou d'un concours, les stagiaires de la formation continue et les auditeurs libres.

Article 17 : Obligations relatives aux usagers

Dans le respect des principes précédemment exposés dans le cadre du présent titre, tous les usagers exercent les libertés à titre individuel et collectif dans des conditions qui ne portent pas atteinte aux activités d'enseignement et de recherche et qui ne troublent pas l'ordre public (articles L141-6 et L811-1 du code de l'éducation), et dans le respect des dispositions du présent règlement intérieur.
Ces libertés reposent pour chacun sur le respect de la liberté de conscience, le droit à la protection contre toute agression physique et morale, la liberté d'exprimer ses opinions dans un esprit de tolérance et de respect d'autrui. Sont strictement interdits : les actes de prosélytisme, les manifestations de discrimination, les incitations à la haine et toute forme de pression physique ou psychologique visant à imposer un courant de pensée religieux, philosophique ou politique, qui s'opposerait au principe de neutralité du service public et de laïcité.
Le port par les usagers de tenues vestimentaires manifestant une appartenance religieuse n'est pas incompatible avec le principe de laïcité et de neutralité du service public applicable dans les établissements d'enseignement supérieur, sauf acte de provocation ou de prosélytisme. Cependant pour certains enseignements et notamment les séances de travaux dirigés, de travaux pratiques ou tout autre enseignement comportant la manipulation de substances ou d'appareils dangereux et/ou nécessitant le port de tenues vestimentaires adaptées, les usagers concernés devront adopter une tenue appropriée aux impératifs d'hygiène et de sécurité. Le non-respect de ces obligations d'hygiène et de sécurité pourra faire l'objet de sanctions.

Le port de tenues ne permettant pas l'identification des usagers lors des examens est également prohibée. En vue de prévenir les fraudes ou tentatives de fraudes, il peut être demandé aux étudiants de se découvrir, de dégager les oreilles afin de s'assurer de l'absence de tout appareil ou équipement de communication au moment de la vérification. L'étudiant peut demander que cette vérification s'opère discrètement. Les oreilles n'ont pas à être dégagées durant tout le déroulement de l'épreuve.
La liberté de conscience est garantie aux usagers. Ils peuvent bénéficier d'autorisations d'absence pour participer à l'une des fêtes religieuses faisant l'objet de la circulaire ministérielle annuelle.

Article 18 : Délit de Bizutage

Toute manifestation à caractère de bizutage, intra ou extra muros, est formellement interdite.
L'article 225-16-1 du code pénal précise que hors les cas de violences, de menaces ou d'atteintes sexuelles, le fait pour une personne d'amener autrui, contre son gré ou non, à subir ou à commettre des actes humiliants ou dégradants ou à consommer de l'alcool de manière excessive, lors de manifestations ou de réunions liées aux milieux scolaire, sportif et socio-éducatif est un délit punissable dans des conditions prévues par ce code.
Indépendamment de la mise en œuvre des poursuites pénales, des poursuites disciplinaires peuvent être engagées à l'égard des auteurs des faits.
En outre, toute personne, s'il est avéré qu'elle a, par son comportement, organisé, encouragé, facilité le bizutage ou si elle s'est abstenue de toute intervention pour l'empêcher, peut également faire l'objet de poursuites disciplinaires.
Le CHSCT doit être tenu informé de toutes les situations de bizutage et peut proposer des moyens d'y remédier. Le Comité d'orientation du Bureau de la Vie Etudiante (BVE) doit être tenu informé de toutes les situations de bizutage et réfléchir aux moyens d'y remédier.

Article 19 : Règles générales de scolarité
(Se reporter au Guide des Etudes, disponible sur l'intranet de l'URCA)

Article 19-1 : Inscriptions et carte d'étudiant

Lors de l'inscription définitive, une carte d'étudiant est délivrée. La carte d'étudiant est un document nominatif et personnel, exclusivement délivré par les services habilités de l'université. Elle doit permettre l'identification rapide et sans ambiguïté des étudiants inscrits.
Une carte de stagiaire de la formation continue dans laquelle il est inscrit sera délivrée à l'étudiant.
La carte d'étudiant et la carte de stagiaire donnent accès aux locaux de l'université et doit être présentée impérativement aux autorités administratives ou agents désignés par elles chaque fois que ceux-ci le demandent.
Elle ne peut être ni cédée, ni prêtée, ni utilisée frauduleusement. Son utilisation frauduleuse est passible de sanctions disciplinaires. Les dates d'inscription doivent être respectées pour assurer un bon fonctionnement de la scolarité et des études.
L'inscription de tous étudiants et autres usagers à l'université ne sera effective que si toutes les conditions réglementaires ont été requises, notamment l'acquittement des droits d'inscription.

Article 19-2 : Calendrier universitaire

Le calendrier est porté à la connaissance des usagers sur le portail numérique de l'université et par voie d'affichage dans les services de la scolarité de l'administration centrale et des composantes.
Les usagers doivent respecter le calendrier universitaire proposé par chaque composante et approuvé par les différents conseils (début et fin des cours et des examens, congés). Les emplois du temps sont affichés dans les services de scolarité et consultables sur le bureau virtuel. En cas de litiges, seul l'affichage sera pris en compte.

Article 19-3 : Stages

Tout stage en entreprise intégré dans un cursus doit faire l'objet d'une convention de stage, conformément à la législation et à la réglementation en vigueur.

L'étudiant reste affilié au régime d'assurance sociale auquel il a souscrit lors de son inscription mais il doit souscrire une assurance responsabilité civile. L'étudiant bénéficie de la protection le garantissant contre les accidents survenant pendant le stage ou sur les trajets inhérents au stage

(R.L.R. 453-1, circulaire n°86-065).

Le maintien de la couverture accident du travail est possible dans le cas de stages obligatoires à l'étranger n'excédant pas l'année universitaire.

Enfin, les étudiants et autres usagers doivent s'informer des modalités pédagogiques du stage (suivi pédagogique, validation, évaluation…) auprès des secrétariats et des enseignants de chaque composante.

Article 19-4: Charte du doctorat

Sous la responsabilité de l'établissement accrédité, chaque école doctorale fixe les conditions de suivi et d'encadrement des doctorants par une charte du doctorat dont elle définit les termes. Cette charte prévoit notamment les modalités de recours à une médiation en cas de conflit entre le doctorant et son directeur de thèse et l'engagement du doctorant à répondre à toute demande d'information relative à son insertion et à son parcours professionnel à l'issue du doctorat. Cette charte est approuvée par chaque directeur d'école doctorale, le directeur de l'unité ou de l'équipe de recherche d'accueil, le ou les directeurs de thèse. Elle est signée par le doctorant et le directeur de thèse lors de sa première inscription. Toute modification de la charte par les conseils d'écoles doctorales doit être portée à la connaissance du CA.

SOUS-TITRE 2 : DISPOSITIONS APPLICABLES AUX PERSONNELS

Article 20 : Notion de personnels

Sont considérées comme personnels les personnes nommées ou affectées à l'université ainsi que les personnes mises à disposition de l'université ou recrutées par l'université.

Article 21 : Obligations relatives aux agents du service public

En règle générale, les droits et obligations des personnels sont ceux que déterminent les textes législatifs et réglementaires qui leur sont applicables et notamment leur statut respectif.

Selon les termes de l'article L952-2 du code de l'éducation, les enseignants-chercheurs, les enseignants et les chercheurs jouissent d'une pleine indépendance et d'une entière liberté d'expression dans l'exercice de leurs fonctions d'enseignement et leurs activités de recherche, sous les réserves que leur imposent, conformément aux traditions universitaires et au code de l'éducation, les principes de tolérance et d'objectivité.

Tout agent public a un devoir de stricte neutralité. Il doit traiter également toutes les personnes et respecter leur liberté de conscience. Le fait pour un agent public de manifester ses convictions religieuses, notamment par le port de tenues manifestant une appartenance religieuse, dans l'exercice de ses fonctions constitue un manquement à ses obligations. Il appartient aux responsables des services publics de faire respecter l'application du principe de laïcité dans l'enceinte de ces services. Les agents publics ne peuvent se livrer, par leurs propos et leur apparence, au prosélytisme, à la propagande ou à la discrimination.

La liberté de conscience est garantie aux agents publics. Ils bénéficient d'autorisations d'absence pour participer à l'une des fêtes religieuses faisant l'objet de la circulaire annuelle ministérielle dès lors que l'absence est compatible avec les nécessités du fonctionnement normal du service.

Dans le cadre de ses missions à l'université, tout intervenant est soumis aux mêmes obligations.

TITRE III : HYGIENE, SECURITE ET ENVIRONNEMENT

Article 22 : Hygiène et sécurité

Le Règlement « hygiène, sécurité, santé, environnement » de l'URCA est disponible en annexe 1 du présent règlement intérieur.

Article 23 : Environnement

L'université est engagée dans une démarche volontariste concernant le développement durable et la responsabilité sociétale (DD&RS). Elle inscrit son action dans tous les domaines qui relèvent de sa compétence : l'enseignement, la recherche, la gouvernance, l'environnement et la politique sociale, avec comme lignes directrices les 17 objectifs de développement durable (ODD) de l'organisation des nations unies (ONU).

Pour opérationnaliser son action, elle s'appuie sur une mission DD&RS rattachée à la direction générale des services ainsi que sur un réseau d'ambassadeurs et d'ambassadrices DD&RS qui seront les relais de la mission dans l'ensemble des composantes, services, directions, unités de recherche et associations étudiantes de l'université.

Le comité de pilotage DD&RS assure la coordination du réseau des ambassadeurs et ambassadrices. Il a pour mission de :

- favoriser l'émulation d'idées de la communauté autour des enjeux DD&RS de l'établissement,
- proposer et accompagner tout ou partie des actions stratégiques et opérationnelles au sein de l'établissement,
- rendre un avis sur sollicitation de la direction, des conseils ou des usagers de l'établissement.

Le comité de pilotage est présidé par le vice-président en charge du DD&RS. Il comprend à minima le ou chargé de mission DD&RS, le vice-président en charge de la vie étudiante, le vice-président étudiant, le directeur de la DPLDD, le directeur de la communication, et la direction générale des services.

TITRE IV : L'ORDRE DANS LES ENCEINTES ET LOCAUX DE L'UNIVERSITE

Article 24 : Accès aux locaux

Les enceintes et locaux universitaires sont accessibles aux personnels, aux usagers, aux personnes participant aux activités pédagogiques, administratives, scientifiques, culturelles ou documentaires de l'université ainsi qu'à toute personne dûment autorisée à titre personnel.
Toute personne présente dans les locaux de l'université doit être en mesure de justifier le caractère régulier de sa présence dans les enceintes et les locaux universitaires, sur demande. Les étudiants doivent être porteurs en permanence de leur carte d'étudiant, et la présenter à la demande. A défaut, ces personnels peuvent demander aux personnes en cause de quitter les lieux sans délai.
L'accès aux locaux de l'université peut être limité lorsque les circonstances l'exigent, notamment pour des raisons de sécurité.

Article 25 : Dispositions relatives aux voies de stationnement sur le campus

Les dispositions du code de la route s'appliquent sur l'ensemble des voies de circulation et aires

de stationnement de tous les campus de l'université. La circulation piétonnière est prioritaire sur le campus universitaire.
Les membres de la communauté universitaire sont tenus de respecter la signalisation relative à la circulation et au stationnement. Il est notamment strictement interdit de stationner sur les voies d'accès des services de secours. Les voies d'accès des pompiers ou de véhicules de secours doivent être dégagées en permanence ; les forces de police peuvent intervenir pour en libérer l'accès. Les contrevenants s'exposent à l'enlèvement de leurs véhicules.

Article 26 : Maintien de l'ordre dans les locaux

Le pouvoir de police administrative appartient au président de l'université, en lien avec les autorités préfectorales.
Le Président de l'université est responsable de l'ordre et de la sécurité dans les enceintes et les locaux affectés à titre principal à l'établissement, et dont il a la charge. Sa compétence s'étend aux locaux mis à la disposition des usagers et du personnel. Le Président est compétent pour prendre toute mesure utile permettant d'assurer le maintien de l'ordre et peut, en cas de nécessité, faire appel à la force publique. En cas de désordre ou de menace de désordre dans les enceintes et locaux, le Président, peut, à titre temporaire, interdire à toute personne l'accès partiel ou total de ces enceintes et locaux ou suspendre des enseignements.

Article 27 : Vidéosurveillance

Il ne doit pas y avoir de surveillance à l'insu des personnes concernées à savoir des enseignants, des étudiants, des personnels et des visiteurs. L'existence d'un système de vidéosurveillance doit être portée à la connaissance de toute personne filmée ou susceptible de l'être de façon claire et permanente par exemple au moyen de panonceaux apposés à l'entrée des locaux.

Les instances représentatives du personnel doivent être consultées avant toute mise en œuvre d'un système de vidéosurveillance et précisément informées des fonctionnalités envisagées.

Les images enregistrées ne peuvent être visionnées que par les seules personnes dûment habilitées à cet effet dans le cadre de leurs attributions respectives.

Sauf enquête ou information judiciaire, la durée de conservation des images enregistrées à l'aide d'un dispositif de vidéosurveillance ne peut excéder un mois et les enregistrements doivent être détruits par la suite.

Un système de vidéosurveillance numérique mis en place dans les enceintes et locaux affectés à titre principal à l'établissement ne peut être installé que s'il a préalablement fait l'objet d'une déclaration auprès de la CNIL. Le traitement des enregistrements est toutefois dispensé de déclaration en cas de désignation d'un Correspondant Informatiques et Libertés.

TITRE V : CHARTE INFORMATIQUE ET MOYENS DE COMMUNICATION

Article 28 : Charte régissant l'usage du système d'information

Les étudiants et autres usagers et personnels appartenant à l'université sont soumis au respect de la charte informatique (annexe 2).

Article 29 : Moyens de communication et respect de l'identité et de l'image de l'université :

L'utilisation des services d'Internet ainsi que du réseau pour y accéder n'est autorisée que dans le cadre exclusif des activités d'enseignement et de recherche des utilisateurs. L'usage de sites

dont le contenu est contraire à l'ordre public et aux bonnes mœurs (sites pornographiques, négationnistes ou à caractère discriminatoire ou diffamatoire et sectaire) est interdit et passible de sanctions pénales et disciplinaires.

Les terminaux mobiles communicants (téléphones mobiles, smartphone, tablette ; tout type de nouvelles technologies et d'enregistrement) sont interdits dans le cade des examens. Dans le cadre des activités pédagogiques, leur utilisation reste soumise à l'autorisation de l'enseignant.

Chaque étudiant ayant une inscription valide dispose d'une adresse courriel institutionnelle propre à l'URCA.

Tout document ou publication émanant d'une structure de l'Université doit faire référence, quel que soit son support, à son appartenance à l'université. Les documents officiels portent obligatoirement le logo de l'Université. Ce logo est à demander à la Direction de la communication (par courriel : direction.communication@univ-reims.fr). L'utilisation du logo de l'université pour tout autre usage doit être soumise à une autorisation préalable du Président de l'Université. Les sites web des composantes de l'université doivent clairement faire mention de leur rattachement à l'université et un lien vers le site de l'université doit être opérationnel.

Article 30 : Reprographie et propriété intellectuelle :

Les personnels et les usagers doivent respecter le code de la propriété intellectuelle (loi 92-597 du 1er juillet 1992) qualifiant de délit la contrefaçon entre autres des ouvrages et des logiciels. Les reproductions, copies, diffusion de documents sont strictement réservées à un usage privé et soumises au respect de la législation en vigueur. L'utilisateur contrevenant est passible de sanctions administratives et sa responsabilité propre peut par ailleurs être engagée, dans les conditions prévues par le code de la propriété intellectuelle, pour toute utilisation non conforme ou illicite.

L'Université de Reims Champagne-Ardenne signe chaque année un contrat d'autorisation de reproduction par reprographie d'œuvres protégées. Les usagers et les personnels doivent en conséquence respecter ce contrat et suivre les recommandations de la « charte pour le respect de la propriété intellectuelle » dans les universités (***charte graphique disponible sur le bureau virtuel*).**

TITRE VI : DISPOSITIONS FINALES

Article 31 : Respect du règlement intérieur

Le présent règlement intérieur s'applique à toutes les structures, composantes et services de l'Université.
Tout manquement à ce règlement intérieur peut entraîner le déclenchement de procédures réglementaires, voire disciplinaires.

Article 32 : Adoption et modification

Le règlement intérieur de l'université est adopté par le conseil d'administration de l'université.
Il est soumis pour avis au Comité technique pour les dispositions relevant des compétences de celui-ci.
Il peut être révisable autant que de besoin en fonction de l'évolution de la vie universitaire et en respectant les mêmes modalités d'approbation.
Il est porté à la connaissance des personnels et des usagers de l'URCA par tout moyen approprié, et, en tout état de cause, par publication sur le site web de l'université et sur l'intranet.

ANNEXE 1

REGLEMENT INTERIEUR RELATIF A L'HYGIENE, LA SECURITE, L'ENVIRONNEMENT ET LA SANTE DES PERSONNELS ET USAGERS DE L'UNIVERSITE DE REIMS CHAMPAGNE ARDENNE

(Décret du 28 mai 1982 modifié – décret du 24 avril 2012 – code du travail livre IV
Règlement de sécurité incendie du 25 juin 1980 modifié des établissements recevant du public)

Préambule : Afin de prévenir tout accident et de garantir de bonnes conditions de vie et de travail pour tous les membres de la communauté universitaire, l'élaboration de règles de fonctionnement est indispensable.
Ce règlement intérieur permet de mettre à portée de toutes les règles définies par la loi en matière d'hygiène, de sécurité, de santé et d'environnement. Toute personne qui ne respecte pas la loi et ce règlement et qui met en danger la vie d'autrui engage sa responsabilité pénale.

Au-delà du simple aspect réglementaire, les sujets développés dans ce document ont pour vocation d'inciter chacun d'entre nous à faire les efforts nécessaires pour le respect de l'autre et le respect des espaces et biens communs. L'inscription en tant qu'étudiant, l'activité professionnelle, même ponctuelle, ainsi que la présence à quel titre que ce soit au sein de l'Université de Reims Champagne Ardenne, impliquent pour chacun l'acceptation et l'application de ces consignes.

1) Règles générales liées à la prévention des risques.

1.1) Partage des responsabilités :
Chacun est responsable de sa propre sécurité mais aussi de celle des autres. La responsabilité peut être engagée pour tout acte ou omission susceptible de mettre autrui en danger ou conduisant à un incident ou un accident.
Les chefs de services sont responsables de la sécurité des personnels et du public, présents dans leurs services. Ils doivent prendre toute disposition utile pour garantir cette sécurité à tout moment.
Un arrêté du président précise les fonctions d'encadrement assimilables à la notion de « chef de service » au sens de la santé et de la sécurité des personnels.
Les enseignants sont responsables de la sécurité des étudiants pendant le face-à-face pédagogique. Ils doivent prendre toute disposition utile pour garantir cette sécurité durant cette période.

1.2) Informations et consignes générales
Afin d'être correctement informés de l'organisation générale de la sécurité au sein de l'Université et de toutes les règles qui s'y appliquent, les personnels et les étudiants sont invités à consulter les pages de l'Intranet du site de l'université accessible depuis le Bureau Virtuel et consacrées à la prévention des risques***.*** En complément, des consignes de sécurité ou règlements intérieurs spécifiques à chaque site et chaque unité de travail, peuvent être édictées dans la mesure où elles ne contredisent pas les règles du présent règlement. Le présent règlement constitue une approche générale des règles de sécurité à respecter. Pour consulter le détail des dispositions règlementaires et consignes à respecter, les personnels sont invités à se référer à la collection des Fiches Pratiques de Sécurité réalisées par le service prévention des risques et disponibles sur l'Intranet ou auprès du service***.***

1.3) Signalétique de sécurité
Une signalétique de prévention, composée d'affiches utilisant des pictogrammes de dangers, d'interdiction, d'obligation etc. est mise en place dans les locaux de l'établissement et plus particulièrement au niveau des locaux à risques (ateliers, laboratoires, locaux techniques) et des équipements et matériels à risques (machines…). La liste et la signification exacte des pictogrammes sont consultables sur l'Intranet ou peuvent être obtenus sur demande au service prévention des risques. Les personnels et les étudiants sont tenus de respecter la signalétique et les consignes. Il appartient aux responsables des locaux concernés, de prendre les mesures nécessaires pour mettre à disposition les équipements de sécurité que la signalétique impose et en cas de non-respect des consignes (l'exclusion du local ou l'interdiction d'usage d'un équipement sont recommandées).

1.4) Droit et devoir d'information :

Les personnels et les étudiants sont tenus d'informer immédiatement les chefs des services ou les personnes compétentes, de toute information ou toute situation observée pouvant conduire à exposer une ou plusieurs personnes à un risque. Des cahiers de santé sécurité au travail sont disponibles sur les sites et doivent pouvoir être consultés librement pour signaler tout problème par écrit. De même, un service d'assistance disponible depuis le bureau virtuel (les tickets prévention) permet le signalement des problèmes par voie électronique. L'absence de signalement d'une situation à risques peut conduire à une condamnation pénale pour non-assistance à personne(s) en danger.

Tout membre de la communauté universitaire a le droit d'obtenir toute information relative à sa propre sécurité au sein des sites de l'Université de Reims Champagne Ardenne.

1.5) Droit et devoir de retrait

Toute personne estimant être exposée à un danger grave et imminent peut faire valoir son droit de retrait. Le droit de retrait doit faire l'objet d'une information immédiate auprès du supérieur hiérarchique direct. Aucune sanction ne pourra être prise envers la personne ayant fait valoir son droit de retrait dès lors que celui-ci est justifié et que la procédure a été respectée. La procédure est décrite sur l'Intranet ou disponible auprès du service prévention des risques.

Lors de situations critiques évidentes, le refus de retrait d'une personne exposée à un danger grave et imminent engagera sa propre responsabilité en cas d'accident.

1.6) Travail isolé

A l'exclusion des activités faisant l'objet d'une interdiction règlementaire dans ce domaine, le travail isolé d'un membre du personnel doit faire l'objet d'une autorisation préalable de l'encadrant en charge de sa sécurité. Le travail isolé ne peut être autorisé qu'après évaluation des risques et de l'opportunité et à partir du moment où les dispositions ont été prises pour permettre à l'agent concerné d'être secouru dans les plus brefs délais en cas d'urgence.

1.*7*) Incidents - Accidents

Tout incident et tout accident, même bénin, concernant les étudiants, les personnels ou toute personne extérieure à l'établissement doit faire l'objet d'une déclaration selon les procédures existantes au sein de l'établissement.

2) Formation sécurité

2.1) Le parcours Prévention pour les personnels et doctorants

Tout nouvel arrivant à l'Université, qu'il soit stagiaire, fonctionnaire ou contractuel, enseignant ou non, est convié à une session de sensibilisation à la sécurité. La participation à cette session de sensibilisation est OBLIGATOIRE. En cas d'impossibilité, la personne doit prévenir le service formations et concours de la Direction des Ressources Humaines afin d'être inscrite à une session ultérieure.

Toute personne travaillant à l'université et n'ayant pas été invitée à suivre cette session de sensibilisation à la sécurité est appelée à s'inscrire auprès du service formations et concours.

Au cours de la formation, les personnes sont classées selon les types de risques auxquels elles sont exposées (Vert : sans risque particulier, Rouge : risque chimique, biologique ou physique, Bleu : catégories spécifiques (ménage – services généraux, conducteurs etc.). Un test permet de valider la formation.

Selon leur classement, elles doivent suivre un complément de formation obligatoire :

- sur les bonnes pratiques de laboratoire pour les personnes classées en « rouge »,
- spécifique à leur activité pour les personnes classées en « bleu ».

Un complément de formation doit être donné localement aux nouveaux arrivants sur leur lieu de travail afin qu'ils en connaissent les spécificités, l'organisation et les risques particuliers. Cette formation est faite sous la responsabilité et à l'initiative des chefs de services concernés.

Le Parcours Prévention s'applique également aux doctorants dans le cadre des écoles doctorales.

2.2) Formations des personnels d'encadrement

En complément de la formation de sensibilisation à la sécurité, chaque participant est amené à indiquer s'il doit assurer une fonction d'encadrement, auquel cas il lui sera proposé un parcours de formation complémentaire spécifique au management.

2.3) Formations techniques spécifiques

Les activités spécifiques suivantes nécessitent obligatoirement l'habilitation des personnes concernées. Cette habilitation est délivrée par le chef d'établissement après avis de l'intervenant ayant assuré la formation. Il est strictement interdit à toute personne ne disposant pas de cette habilitation d'exercer ces activités. Il s'agit de :

- Tout travail exposant à des risques électriques (différents niveaux d'habilitation nécessaire)
- Tout travail exposant à des rayons X ou des rayonnements ionisants (personne radio-compétente)
- Tout travail sur appareil à pression soumis à contrôle périodique (qualification nécessaire)
- Toute manipulation d'animaux (agrément nécessaire)
- Toute conduite de véhicule sans disposer du permis approprié (voitures – chariots élévateurs, nacelles…)

Les personnes en infraction par rapport à cette règle sont invitées à contacter de toute urgence le service formations concours pour une régularisation de leur situation.

2.4) Formation à la sécurité des étudiants

En fonction du cursus et des activités des étudiants, les enseignants et responsables de départements d'enseignement sont tenus de transmettre par voie orale et écrite aux étudiants toute information utile pour leur sécurité. Pour les séances de travaux pratiques, la signature par chaque étudiant de la charte de sécurité de l'étudiant en TP est vivement recommandée (disponible sur l'Intranet ou sur demande auprès du service prévention des risques).

3) Evaluation des risques professionnels

3.1) Document Unique d'Evaluation des Risques

Chaque unité de travail doit réaliser son document unique d'évaluation des risques (DUER). Le DUER est constitué de plusieurs parties :

- Un inventaire des risques auxquels sont exposés les personnels de l'Unité de travail. Cet inventaire doit être hiérarchisé. Chaque risque est évalué en fonction de plusieurs critères (nombre de personnes exposées, durée d'exposition, gravité en cas d'accident, maîtrise du risque etc.). Lorsqu'il est indiqué que les risques sont maîtrisés, la façon dont ils sont maîtrisés doit être développée
- Un bilan de l'organisation sécurité de l'unité de travail
- Un bilan de la formation sécurité et du suivi médical des agents de l'Unité de travail
- Un plan d'action précis, qui indique les actions à mettre en œuvre pour supprimer, diminuer ou maîtriser les risques inventoriés. Ce plan doit clairement préciser les délais pour la réalisation de l'action et le nom de la personne chargée de veiller à ce qu'elle soit réalisée.

Le DUER doit être signé par le chef de l'unité de travail et mis à jour au moins une fois par année universitaire.

3.2) Fiche Individuelle d'Exposition aux Agents Chimiques Dangereux

Tout agent exposé dans le cadre de son activité à des agents chimiques dangereux est tenu de compléter une fiche individuelle d'exposition aux agents chimiques dangereux. Cette fiche est archivée au service prévention des risques et transmise au service de médecine de prévention pour information et associée au dossier médical de l'agent. La fiche doit faire l'objet d'une mise à jour annuelle au minimum. Cette fiche confidentielle est mise à jour annuellement avec conservation des fiches antérieures en vue de permettre une traçabilité de l'évolution de l'exposition aux risques tout au long de la carrière de chaque membre du personnel au sein de l'URCA.
L'étude des différentes fiches permettra de remettre à chaque agent qui quitte l'URCA, son attestation d'exposition aux risques professionnels au poste de travail. Elle permettra également la réalisation des fiches collectives de risques prévues par la réglementation.

3.3) Fiches individuelles d'Exposition à d'autres risques professionnels

En complément de la fiche réglementaire prévue au paragraphe 3.1, des fiches individuelles d'exposition aux risques supplémentaires peuvent être réalisées en fonction des risques auxquels est exposé chaque agent.

4) Suivi médical des personnels et des étudiants

4.1) Visites médicales obligatoires pour les personnels et doctorants

Tous les personnels, enseignants et non enseignants, sont tenus de se rendre aux visites médicales auxquelles ils sont convoqués. En cas de force majeure, toute annulation de visite doit se faire au plus tard la veille de la date fixée. Les personnels peuvent demander à bénéficier d'une visite médicale sans attendre leur convocation automatique, sur simple demande auprès du service prévention des risques. La visite médicale permet de dresser un bilan des

risques professionnels auxquels sont exposés les personnels dans le cadre de leur travail. Il s'agit d'évaluer les effets indésirables que peut avoir le travail sur le capital santé des agents.

En fonction du bilan d'exposition aux risques professionnels, les personnels bénéficient soit d'une surveillance médicale normale, soit d'une surveillance médicale renforcée :

- Surveillance médicale normale : Visite médicale obligatoire tous les 5 ans.
- Surveillance médicale renforcée : Visite médicale obligatoire tous les ans. Le suivi médical est obligatoirement assuré par ~~le~~ un service de médecine de prévention lié par convention avec l'Université.

4.2) Suivi médical pour les étudiants

Le suivi médical des étudiants est assuré par le service de médecine préventive. Ce dernier réalise également des campagnes de prévention sur les thématiques concernant les étudiants.

5) Sûreté - Sécurité incendie – Evacuation – Mise à l'abri

5.1) Accès et présence sur les sites et dans les locaux de l'URCA

Chaque site précise dans son règlement intérieur les horaires et conditions d'accès au site et aux bâtiments selon l'activité du bâtiment et les personnes concernées (public – étudiants – personnels).
L'ouverture au public d'un site implique obligatoirement la présence ou la possibilité d'intervention rapide du responsable de sécurité du site ou de son représentant pour prendre les premières mesures de sécurité qui s'imposent en cas d'urgence.

Toute personne présente dans l'enceinte de l'URCA doit être en mesure de justifier de son identité sur demande d'un membre du personnel de l'établissement. Cette justification se fait par la présentation de la carte d'étudiant, de la carte professionnelle, ou à défaut d'une pièce d'identité. Toute personne qui se refuse à cette demande de justification sera invitée à quitter immédiatement le site ou les locaux. A défaut elle fera l'objet d'un signalement aux autorités de police.

Sauf nécessité absolue liée à la sécurité des personnes, il est strictement interdit de favoriser l'accès à un bâtiment par la neutralisation des dispositifs de contrôle d'accès lorsqu'ils existent.

5.2) Respect du matériel

Les installations et équipements de sécurité incendie (extincteurs, systèmes d'alarme…) ont pour but de préserver la vie des personnels et du public en cas de sinistre. Ces matériels qui peuvent sauver des vies doivent être respectés et maintenus en bon état de fonctionnement.

5.3) Evacuation des locaux en cas de nécessité

L'organisation périodique d'exercices d'évacuation dans les locaux de l'Université est une obligation réglementaire. Ces exercices permettent également aux personnels et au public de se familiariser avec les sirènes d'alarme et les cheminements d'évacuation. Leur périodicité est fixée à 2 par bâtiment et par année universitaire. Dès audition de l'alarme et dans tous les cas, les locaux doivent être immédiatement évacués selon les consignes prévues à cet effet. Les personnes évacuées doivent suivre les instructions des chargés d'évacuation et rejoindre le point de rassemblement le plus proche. La participation aux exercices est obligatoire.

5.4) Prévention du risque d'incendie

Il appartient à chacun, à chaque instant, de veiller par son comportement et son activité à la prévention du risque d'incendie. Cette prévention passe notamment par l'utilisation avec précaution des produits inflammables dans les laboratoires et ateliers, la délivrance de permis de feu préalablement à tous travaux présentant des risques d'incendie, et l'interdiction de fumer dans l'ensemble des locaux. Il est également demandé de ne jamais laisser des appareils électriques (ordinateurs, photocopieurs, cafetières…) sous tension de façon prolongée et en l'absence de surveillance (sauf équipements particuliers).

5.5) Mise à l'abri en cas de nécessité

Lors d'une situation de risque majeur (accident technologique ou tempête), la protection des personnels et des usagers est nécessaire par une mise à l'abri dans les locaux. L'organisation de la gestion de ces situations est définie dans les Plans Particuliers de Mise en Sécurité progressivement mis en place sur les sites de l'Université. Lorsque des exercices sont organisés, la participation des personnes présentes est obligatoire.

6) Cadre de vie

Afin de garantir à tous à tout moment un cadre de travail et de vie satisfaisant et respectueux des libertés de chacun, il est indispensable de se soumettre à des règles de vie en communauté.

6.1) Hygiène générale

Par respect des autres et plus particulièrement du personnel chargé de l'entretien, les personnels et les étudiants sont tenus de laisser les locaux en état de propreté. Chaque personne présente dans l'enceinte de l'URCA est tenue de respecter un minimum de règles d'hygiène corporelle et vestimentaire pour le confort de tous.

6.2) Tabagisme *(modifié par délibération du CHSCT du 13 juin 2013)*

L'interdiction de fumer s'applique dans l'ensemble des espaces clos et couverts de l'établissement, qu'ils soient privés ou publics, à l'exception des appartements des personnels logés. Les mêmes conditions d'interdiction s'appliquent également à l'usage de la cigarette électronique.

6.3) Consommation de stupéfiants

L'introduction et la consommation de stupéfiants dans l'enceinte de l'Université (extérieur – intérieur) sont strictement interdites. L'entrée ou la présence dans l'enceinte de l'établissement d'une personne manifestement sous l'emprise d'un produit stupéfiant doit être immédiatement signalée au responsable de site qui se chargera d'assurer son évacuation par les services de secours (pompiers).

6.4) Alcool

La vente d'alcool est interdite. Des dérogations peuvent être obtenues sur demande pour des manifestations spécifiques (soirées étudiantes, vente en cafétéria CROUS pendant les repas…). Elles seront limitées aux boissons dont la consommation est tolérée par le code du travail (vins, bière, cidre, poiré et hydromel, non additionnés d'alcool).

La consommation d'alcool sur le lieu de travail est également interdite. Une tolérance limitée aux alcools cités dans le paragraphe ci-dessus est acceptée pour une consommation au cours des repas et en cas de manifestations particulières (colloques, pots de thèse, de départ, de fin d'année…). La consommation doit se faire avec modération et les quantités proposées doivent être en adéquation avec le nombre de participants. En tout état de cause, des boissons non alcoolisées devront être obligatoirement proposées en quantité suffisantes. Il appartient à l'organisateur de la manifestation de prendre les dispositions nécessaires pour prévenir tout risque consécutif à un état d'ébriété et notamment de conduite en état d'ivresse.

L'entrée ou la présence dans l'enceinte de l'établissement d'une personne manifestement en état d'ébriété doit être immédiatement signalée au responsable de site qui se chargera d'assurer son évacuation par les services de secours (pompiers).

6.5) Ambiance thermique

Tout personnel et usager est en droit d'exiger de pouvoir travailler dans de bonnes conditions de température.

Les situations d'exposition des personnels aux fortes chaleurs doivent être traitées au cas par cas avec le supérieur hiérarchique. L'exposition à des températures anormalement basses par rapport à la situation normale de travail, doit également faire l'objet d'un aménagement avec le supérieur hiérarchique.

6.6) Ambiance sonore

Le port de protections auditives est obligatoire pour tout travail dans un espace dans lequel les valeurs d'exposition au bruit dépassent 85 dB(A). Les protections individuelles sont obligatoirement mises à disposition lorsque le bruit dépasse 80 dB(A). Lorsque le bruit constitue une gêne sans dépasser les valeurs limites, une étude d'aménagement de poste ou d'organisation du travail doit être menée.

Afin de respecter le silence nécessaire au travail ou aux études il est demandé aux usagers et personnels de couper la sonnerie de leur téléphone portable lorsqu'ils entrent dans les salles, les bibliothèques ou les bureaux. L'écoute de musique et les conversations doivent se faire à un niveau sonore n'entraînant pas de gêne pour les autres.

6.7) Animaux

La présence d'animaux de compagnie est formellement interdite dans tous les locaux de l'université, sauf dans les cas suivants, s'ils ne perturbent pas la sécurité de l'activité et sont tenus en laisse :

- appartenant au personnel logé pour raison de service
- appartenant aux agents de gardiennage
- servant de guide ou d'aide à une personne handicapée

Pour des raisons d'hygiène, il est interdit de nourrir les animaux errants sur les sites.

6.8) Circulation

L'ensemble des règles du code de la route s'applique au sein des sites de l'Université, y compris pour les piétons et les cyclistes. La vitesse maximale est limitée à 30 km/h. Elle peut être inférieure à cette valeur dans certaines zones signalées. L'établissement se réserve le droit de faire intervenir la force publique pour procéder notamment à des contrôles de vitesse. La circulation au sein des sites est limitée à l'accès aux parkings. Les autres voies de circulation sont réservées aux piétons, aux véhicules de service et de livraison et à titre exceptionnel aux titulaires d'une autorisation spéciale.

La circulation hors des voies normales, notamment sur les espaces verts est strictement interdite sauf autorisation exceptionnelle et justifiée du responsable de site.

L'usage de tout moyen de déplacement mobile (rollers, planches à roulettes, vélos, trottinettes…) à l'intérieur des bâtiments est strictement interdit, à l'exception des équipements pour les personnes handicapées.
Les déplacements à caractère professionnel en voiture de service ou en véhicule personnel impliquent également le strict respect du code de la route. En cas d'infraction, les peines sont à la charge du conducteur. L'usage du véhicule de service implique une vérification préalable de son état général. Les personnels amenés à utiliser leur véhicule personnel dans le cadre d'un déplacement professionnel (en dehors du trajet domicile – travail) doivent veiller à ce que leur assurance couvre ce type de déplacement. Elles doivent faire la preuve qu'elles disposent encore d'un permis de conduire valable au moment de l'utilisation d'un véhicule de service ou du véhicule personnel dans le cadre d'une mission confiée par l'administration.

L'établissement décline toute responsabilité en cas d'accident consécutif au non-respect des règles.

6.9) Stationnement

Le stationnement est limité aux emplacements autorisés et prévus à cet effet. Il est demandé aux usagers et personnels non concernés de ne pas occuper les places réservées aux personnels handicapés, aux deux roues et aux besoins du service. Tout stationnement en dehors des espaces prévus pourra faire l'objet d'un avertissement, qui pourra être suivi d'une immobilisation du véhicule par un sabot en cas de récidive, voire de l'enlèvement du véhicule par la fourrière si son emplacement peut compromettre la sécurité en cas d'évacuation ou d'intervention des secours.
Le cas échéant, les étudiants sont priés de ne pas se garer sur les emplacements réservés aux personnels. Le non-respect de cette règle peut entraîner les mêmes sanctions que celles indiquées ci-dessus.
Il est recommandé de ne pas laisser en évidence dans sa voiture des objets de valeur.

6.10) Travail en dehors des heures normales

L'accès aux sites et bâtiments de l'université en dehors des plages horaires d'ouverture normales (ces plages peuvent varier d'un site à l'autre et sont précisées dans les fiches de consignes générales de sécurité de chaque site) est toléré dans la mesure où il fait l'objet d'une demande d'autorisation justifiée auprès du responsable du site. Une information doit être faite auprès de la personne de permanence. Les règles de sécurité relatives au travail isolé doivent être respectées.

6.11) Mise à disposition de locaux à des tiers

La mise à disposition ponctuelle, périodique ou permanente de locaux de l'Université à des tiers (associations, entreprises, organismes) doit faire l'objet de la signature d'une convention d'occupation précaire du domaine public. Le modèle de convention, qui inclut les questions relatives à la prévention des risques, est disponible auprès de l'administration de l'université.

6.12) Manifestations à caractère exceptionnel

Les locaux de l'Université accessibles au public sont avant tout destinés à l'enseignement.
Toute manifestation autre, qu'elle soit organisée par l'établissement ou des tiers, doit faire l'objet d'une déclaration préalable (article GN6 de la réglementation des établissements recevant du public). La procédure à suivre, les conditions et les dossiers de demande à compléter sont présentées sur l'Intranet et disponibles auprès du service prévention des risques.

6.13) Respect mutuel

Conformément au respect des règles régissant les droits et obligations des fonctionnaires et agents publics, chacun est tenu de respecter à chaque instant ses interlocuteurs au sein de l'URCA. La courtoisie et le respect doivent prévaloir y compris lors de désaccords entre personnes. Les outrages, insultes et injures, oraux ou écrits, sont proscrits et sont susceptibles d'entraîner des poursuites pour leur auteur.
La nécessité de respect mutuel concerne les étudiants entre eux, les personnels entre eux mais également les personnels vis-à-vis des étudiants et vice-versa, ainsi que les relations avec les intervenants de société extérieures au sein de l'URCA.

6.14) Risques Psycho-sociaux

Toute personne qui s'estime victime d'une situation à Risques Psycho-sociaux entraînant un stress ou un mal-être au travail, doit en informer son supérieur hiérarchique. Elle peut également en informer un représentant des personnels, la personne référente de la Direction des Ressources Humaines du Service des Ressources Humaines sur cette thématique, le conseiller de prévention ainsi que le médecin de prévention ou l'assistante sociale.

Toute forme de comportement susceptible de constituer un délit de harcèlement est interdite par la loi et expose leurs auteurs à des sanctions pénales, civiles et administratives. Toute personne qui présume en être victime peut en faire état des référents cités ci-dessus. En cas de danger grave et imminent, toute personne témoin d'une situation de mal-être au travail doit en faire le signalement.

7) Développement durable et protection de l'Environnement

Le respect de l'environnement contribue également à la garantie de bonnes conditions de travail et de vie en communauté. Plusieurs règles sont à respecter à ce titre.

7.1) Gestion des déchets des laboratoires

Les déchets produits par l'activité des laboratoires sont à caractère dangereux (déchets chimiques, radioactifs, biologiques, cadavres d'animaux, éventuellement restes humains et liquides physiologiques, déchets d'activités de soins…). Leur élimination ne doit se faire que par des moyens autorisés et réglementés. Ces filières d'élimination existent au sein de l'Université. Les procédures à suivre sont présentées sur Intranet et disponibles sur demande auprès du service prévention des risques. Il est strictement interdit d'éliminer des déchets liquides dangereux dans les éviers. L'élimination de déchets dangereux avec les déchets banals est également interdite. Les déchets coupants, tranchants (exemples aiguilles de seringues) doivent être conditionnés dans des récipients conformes et inviolables.

7.2) Déchets de verre

L'élimination des déchets de verre doit se faire par la filière prévue à cet effet. La verrerie de laboratoire peut également suivre cette filière uniquement dans le strict respect de toutes les conditions suivantes :

- Verrerie correctement rincée et propre
- N'ayant pas contenu de produit toxique ou poison (symbole « tête de mort »)
- N'ayant pas été en contact avec des produits biologiques

7.3) Déchets informatiques

Les déchets et consommables informatiques sont également des déchets dangereux et leur élimination au titre des ordures ménagères est interdite.

Les cartouches d'encre vides doivent être rendues au fournisseur lors de l'obtention d'une cartouche pleine. Le matériel informatique doit être éliminé par une filière autorisée après sortie des inventaires.

7.4) Papiers – cartons

Les personnels et usagers sont invités à trier leurs déchets afin de permettre le recyclage des papiers et cartons. Des « boites à papier » sont mises en place afin de séparer ces déchets des autres déchets banals.

7.5) Chasse au gaspillage – économies d'énergie

Il est demandé à tous de contribuer activement aux économies d'énergie et de consommables dans un souci de protection de l'environnement.

Des économies de papier peuvent être obtenues en privilégiant l'envoi de courriers par voie électronique, en utilisant des enveloppes à usage multiple pour le courrier interne, en imprimant uniquement les documents nécessaires et en réalisant des impressions en recto- verso et en utilisant les feuilles imprimées sur une seule face pour la réalisation de blocs brouillons.

Lorsque l'on quitte son lieu de travail il est demandé de couper tous les appareils électriques ainsi que l'éclairage et de baisser le chauffage dans la mesure du possible. Les appareils électriques et particulièrement les écrans d'ordinateurs et photocopieurs ne doivent pas être laissés en veille. Ne pas laisser de façon simultanée les fenêtres ouvertes et les radiateurs en marche en période de froid. Utiliser la climatisation de façon limitée.

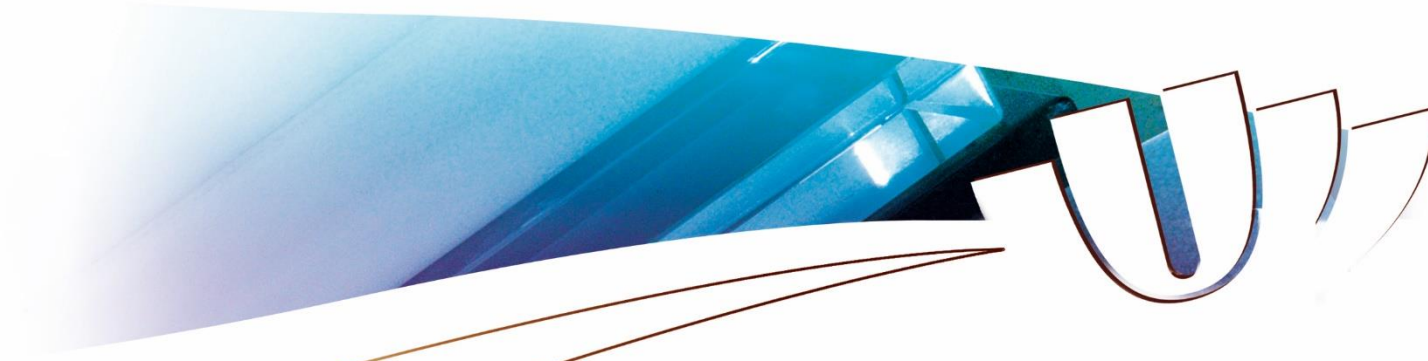
Toute fuite d'eau constatée doit être immédiatement signalée en vue d'être réparée.

8) En cas de non-respect des règles

L’élaboration d’un règlement intérieur de prévention des risques nécessite obligatoirement de prévoir les situations où les règles établies ne sont pas respectées.
Les personnels et étudiants de l’Université doivent savoir que le non-respect des règles peut entraîner selon la situation, des sanctions de différents types. Ces sanctions peuvent être d’ordre administratif ou disciplinaire. Dans certains cas elles peuvent prendre la forme de sanctions de police (ex : non-respect du code de la route) ou de sanctions pénales et civiles, notamment dans les cas où le non-respect des règles entraîne la mise en danger d’autrui ou des dommages matériels et corporels.
Représentants de l’autorité de police du président d’université sur les sites, les responsables de la sécurité des sites ont la responsabilité de l’application des consignes édictées dans le présent règlement.

****

ANNEXE 2



Charte de sécurité de l'Administrateur Informatique au sein de l'Université de Reims Champagne-Ardenne

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

SOMMAIRE

Préambule

Ce document a pour objet de formaliser les règles de déontologie et de sécurité concernant les Administrateurs ou personnels ayant des fonctions spécifiques sur les Systèmes d'Information de l'Université de Reims Champagne-Ardenne (URCA). Dans le cadre de son activité, l'Administrateur pourra être amené à avoir accès aux informations des autres utilisateurs des réseaux, ainsi qu'à des sources d'informations confidentielles.

Le respect de la charte doit s'imposer naturellement à tous les Administrateurs, dans l'intérêt de la communauté des personnes travaillant au sein de l'URCA.

Afin de conduire les actions quotidiennes d'administration et d'exploitation informatique afférentes à sa mission (configuration, supervision, maintenance, évolution, support, ...), l'Administrateur Informatique est doté de droits d'accès privilégiés sur les ressources du SI.
Les risques associés à ces droits d'accès privilégiés peuvent être :

L'accès à des informations dont il n'est pas destinataire, certaines étant confidentielles (bases de données, documents sur les postes de travail utilisateurs, ...) ou à caractère personnel (courriels, fichiers personnels des utilisateurs, ...) ou encore relatives aux activités des utilisateurs et de l'Internet, les données de connexion aux ressources du Système d'Information,
La réalisation des actions potentiellement dangereuses pour la sécurité du Système d'Information : modification ou contournement de mécanismes de protection, création ou modification de comptes utilisateurs, destruction ou modification de fichier, …

En raison de leurs prérogatives, les **Administrateurs** Informatiques ont un rôle essentiel, requérant responsabilité et discrétion. Leur démarche se doit d'être impartiale, leurs interventions ne doivent pas outrepasser leurs attributions ni relever d'actions effectuées pour leur propre compte ou par intérêt personnel.
La présente charte a pour objectif de préciser les droits et devoirs de l'Administrateur Informatique dans l'exercice de sa fonction ou de son activité professionnelle.
Les dispositions de cette charte ne font pas obstacle aux droits et obligations des fonctionnaires.

Article I. Principe et champ d'application

Les règles et procédures de sécurité prévues par la présente Charte s'imposent, dans la limite de leurs attributions effectives, à toutes personnes chargées de l'exploitation, de la maintenance, du suivi de l'utilisation des ressources informatiques et télécommunications et de la mise en œuvre des logiciels.

Ces personnes sont dénommées ci-après les ou l'« Administrateur(s) ».

Article II. Conditions d'utilisation des systèmes d'information

Les moyens mis à la disposition de l'Administrateur sont exclusivement des outils professionnels.
Leur mise à disposition nécessite le respect, par les Administrateurs, de règles essentielles telles que :

- Le respect de la confidentialité absolue des données échangées dans le cadre de leur activité tant à l'égard des tiers qu'à l'égard des autres personnes de l'établissement,

- Le respect des lois et règlements en vigueur.

L'Administrateur est, par ailleurs, soumis à la charte des utilisateurs, de même qu'aux droits et obligations des fonctionnaires.

Article III. Principes de sécurité

La sécurité de ces moyens informatiques et de télécommunications impose aux Administrateurs :

- De garder strictement confidentiel leurs propres mots de passe « Administrateur » sous réserve des dispositions prévues au paragraphe « Continuité de service » de la présente annexe,

- De veiller au respect, par les utilisateurs, des consignes de sécurité figurant dans la charte des utilisateurs,

- D'avertir leur hiérarchie de tout dysfonctionnement constaté et de toutes anomalies,

- De ne pas installer et ne pas utiliser sur les ordinateurs et plus généralement sur les matériels informatiques un logiciel et/ou un progiciel sans qu'une licence d'utilisation appropriée n'ait été préalablement souscrite,

- De n'utiliser que les matériels mis à disposition par la DN, par la direction de la composante/UFR ou de l'établissement,

- De mettre en œuvre les bonnes pratiques en matière de sécurité des SI (droits utilisateurs, réaliser des tests de vulnérabilités, etc.).

Article IV. Gestion des traces – Communication des informations

L'Administrateur assure la gestion des traces et des logs des systèmes d'informations.

Il duplique et assure pendant la durée de conservation prévue, la sauvegarde et la conservation des traces et des logs, prévues par la déclaration d'avis auprès de la CNIL.

La hiérarchie pourra être amenée à demander, sur réquisition de l'autorité judiciaire, aux Administrateurs qu'ils communiquent toutes informations qu'ils pourraient obtenir dans l'exercice de leurs fonctions. Dans le cas d'information dite **nominative** (données à caractère personnel), ces informations ne pourront être communiquées qu'après accord des RSSI (Responsable de la Sécurité des Systèmes d'Information) et du DPO.
Pour rappel, la durée maximale des logs est d'un an. Un administrateur doit pouvoir visualiser des logs jusqu'à trois mois, au-delà seul les RSSI sont autorisés à y avoir accès.

Article V. Droits et Devoirs

Tout administrateur a le droit :

Dans le cadre strict des missions qui lui sont confiées et du respect des mesures de sécurité de la PSSIE [1];

- D'être informé par sa hiérarchie des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible,
- De mettre en place des moyens permettant de fournir des informations techniques d'administration des éléments du système d'information à sa charge (métrologie, surveillance...),
- De mettre en place toutes procédures appropriées pour vérifier la bonne application des règles de sécurité de la PSSIE, en utilisant des outils autorisés,
- D'accéder, sur les systèmes qu'il administre, à tout type d'informations, uniquement à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations, sans les altérer - tant que la situation ne l'exige pas,
- D'établir des procédures de surveillance de toutes les tâches exécutées sur le système dont il a la responsabilité, afin de déceler les violations ou les tentatives de violation de la présente charte et de la charte d'usage du système d'information, sous l'autorité du RSSI et du DPO,
- D'utiliser des outils du système d'information dont la conformité au RGPD et l'information aux personnes concernées ont été effectuées peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire, de suivi fonctionnel, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable,
- De prendre des mesures conservatoires techniques et/ou matérielles, sans préjuger des sanctions résultant des infractions aux différentes chartes, quand il estime qu'une urgence impose de protéger l'intégrité, la disponibilité ou la confidentialité d'un service du système d'information,
- De ne pas intervenir sur un composant hors du système d'information (interne ou externalisé) de l'établissement et hors d'un système d'information confié à l'établissement par convention avec un partenaire, sauf à l'isoler du réseau de l'établissement en cas de besoin.

Tout administrateur a le devoir :

- De respecter les dispositions légales et réglementaires concernant le système d'information, et pour se faire, de se renseigner, si nécessaire, auprès de sa hiérarchie, de la chaîne fonctionnelle SSI, ou du service juridique de l'établissement,
- De respecter la confidentialité des informations auxquelles il accède lors de ses tâches d'administration ou lors d'audit de sécurité, quel qu'en soit le support (numérique, écrit, oral...), en particulier :
    - Les données à caractère personnel contenues dans le système d'information,

[1] PSSIE : https://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf

- Les fichiers utilisateurs,
- Les flux sur les réseaux,
- Les courriers électroniques,
- Les mots de passe,
- Les sorties imprimantes,
- Les traces des activités des utilisateurs.

- De n'effectuer des accès aux contenus marqués comme « privés » qu'en présence de l'utilisateur ou avec son autorisation écrite, à l'exception des cas d'atteinte à la sécurité ou à la disponibilité des d'informations indispensables à la continuité du service sous couvert d'autorisation de la chaîne SSI. Cette obligation ne concerne pas l'utilisation d'outils automatiques qui ne visent pas individuellement l'utilisateur (antivirus, inventaire logiciel, logiciel de sauvegarde...),
- D'être transparent vis-à-vis des utilisateurs sur l'étendue des accès aux informations dont il dispose techniquement de par sa fonction,
- D'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le responsable fonctionnel,
- De garantir la transparence dans l'emploi d'outils de prise en main à distance ou toute autre intervention sur l'environnement de travail individuel de l'utilisateur (notamment en cas d'usurpation de l'identité de l'utilisateur) : limitation de telles interventions au strict nécessaire avec accord préalable de l'utilisateur,
- De s'assurer de l'identité et de l'habilitation de l'utilisateur lors de la remise de tout élément du système d'information (information, fichier, compte d'accès, matériel...), en collaboration avec le responsable fonctionnel,
- De se conformer aux mesures de sécurité de la PSSIE,
- De répondre favorablement, et dans les délais les plus courts, à toutes consignes de surveillance, de recueil d'information et d'audit émis par le RSSI,
- De traiter en première priorité toute violation des règles SSI et tout incident de sécurité qu'il est amené à constater, puis d'informer sans délai le correspondant de sécurité informatique ou le RSSI selon la procédure prévue par la chaîne fonctionnelle de sécurité, et d'appliquer sans délai les directives du RSSI pour le traitement de l'incident. L'administrateur peut ainsi être conduit à communiquer des informations confidentielles ou soumises au secret des correspondances dont il aurait eu connaissance, si elles mettent en cause le bon fonctionnement des systèmes d'information ou leur sécurité, ou si elles tombent dans le champ de l'article 40 alinéa 2 du code de 3 procédure pénale,
- De mettre en œuvre une gestion du cycle de vie des comptes utilisateurs dans les applicatifs qu'il gère.

Article VI. Continuité de service

En toutes circonstances, la continuité du service et de la mission de l'Administrateur doit être assurée.

L'Administrateur doit donc faire le nécessaire pour que soit assuré cette continuité. L'Administrateur doit communiquer ses accès au sein de son service afin d'assurer une continuité d'administration des services quelles que soient les raisons (en cas de départ, de longues absences, …)

Article VII. Confidentialité

L'Administrateur est une personne ayant des droits tout particulièrement étendus quant à l'utilisation et la gestion des systèmes d'information. Cela implique notamment de :

- Ne transmettre aucune information confidentielle sans concertation préalable avec sa hiérarchie et accord du RSSI,
- Dans le cas de toute demande d'information à caractère **nominative** celle-ci devrait faire l'objet au préalable de l'accord du RSSI,
- Veiller à ce que les tiers non-autorisés n'aient pas connaissance de telles informations,
- Respecter ses engagements de confidentialité et de non-divulgation. Il ne fait pas état et n'utilise pas les informations qu'il peut être amené à connaître dans le cadre de ses fonctions,
- Ne pas se connecter à une ressource du SI sans autorisation explicite de la personne à qui elle est attribuée, notamment dans le cas de l'utilisation d'un logiciel de prise de main à distance sur un poste de travail utilisateur,
- Ne pas abuser de ses privilèges, et limite ses actions aux ressources informatiques dont il a la charge, dans le respect de la finalité de sa mission. En particulier, il ne modifie les configurations et les droits d'accès que dans le respect de procédures d'administration ou d'exploitation définies,
- Respecter, d'une manière générale, les règles d'éthique professionnelle, de déontologie, l'obligation de réserve ainsi que le devoir de discrétion.

Dans le cas où un incident de sécurité se produit :

- Il informe son responsable hiérarchique - et selon le cas, le RSSI de l'URCA - de toute faille ou incident de sécurité qu'il pourrait découvrir ou dont il pourrait avoir connaissance,

- Il préserve, conserve et sauvegarde les « traces » nécessaires à la résolution de l'incident et à toute investigation ultérieure, y compris judiciaire, dans des conditions permettant de garantir la valeur probante des « traces ».

Article VIII. Droits d'accès

L'Administrateur s'assure de la protection des droits d'accès liés à sa fonction :

- Il observe les règles de sécurité en vigueur visant à protéger l'utilisation des comptes et des privilèges qui lui ont été attribués. Il veille notamment à la protection des postes de travail à partir desquels il exerce ses fonctions et à la gestion des identifiants et authentifiant des comptes privilégiés. En particulier, les mots de passe utilisés pour les opérations d'administration doivent être robustes et changés régulièrement, conformément à la Politique de Sécurité du SI de l'URCA. Il est rappelé que les droits confiés à un administrateur (et par conséquent les couples identifiants/authentifiant associés) sont personnels et incessibles.

- Il n'utilise les comptes privilégiés que pour les activités et besoins directement liés aux tâches d'administration ou d'exploitation dont il a la charge, étant donné que toute action sur les Systèmes d'Information doit faire l'objet d'une journalisation permettant leur imputabilité.

Article IX. Droit de propriété

L'utilisation des systèmes d'informations implique le respect des droits de propriété de nos partenaires et plus généralement des tiers.

Chaque Administrateur doit donc veiller à ce que :
- Les logiciels soient utilisés dans les conditions de licences souscrites,
- Les logiciels, bases de données, pages Web ou autres créations de tiers protégées par le droit d'auteur ou un droit privatif ne soient pas reproduits, utilisés ou remis à des tiers.

Article X. Délégué à la Protection des Données (DPO)

Tout traitement automatisé de données à caractères personnelles doit faire l'objet d'une déclaration préalable auprès du DPO. (Délégué à la protection des Données) de l'Université à dpo@univ-reims.fr.
L'Administrateur a l'obligation d'alerter le DPO et le RSSI en cas de violation de données à caractère personnel.

Article XI. Responsable Sécurité des Systèmes d'Information (RSSI)

L'Administrateur est tenu d'appliquer sans délai les mesures conservatoires demandées par le RSSI.
Le RSSI est garant des respects de cette charte par les Administrateurs. L'adresse de contact pour écrire au RSSI est rssi@univ-reims.fr.

Article XII. Acceptation des procédures spécifiques aux administrateurs

L'Administrateur Informatique s'engage à respecter en toutes circonstances la législation en vigueur et les règles de la présente charte. En cas de non-respect de la législation en vigueur et des dispositions de la présente charte, l'Administrateur Informatique sera tenu responsable de ses actes et pourra encourir les sanctions prévues dans le Règlement Intérieur de l'URCA ainsi que toute autre sanction civile ou pénale prévue par la loi.

Article XIII. Cas particulier de l'administrateur local

Une partie de l'administration vous est déléguée afin de faciliter l'exploitation de la machine mise à votre disposition. Un compte d'administration local (dont vous possédez le mot de passe) vous permet d'installer des applications et des périphériques supplémentaires. Il autorise également la modification de la configuration du réseau pour utiliser votre ordinateur sur d'autres réseaux.
En contrepartie, l'administrateur local s'engage :

- À ne pas désinstaller ou désactiver les applications préalablement installées par la DN,
- À ne pas créer, modifier ou supprimer les comptes locaux existants (root, administrateur...),

- À ne pas modifier les paramètres système (nom de la machine, stratégies de groupe, paramètres de l'antivirus...),
- À ne pas installer de contenus dont vous ne possédez pas la licence,
- À ne pas divulguer le mot de passe du compte d'administration local,
- À travailler sous le compte administrateur local exclusivement pour la gestion de la machine,
- À connecter sur le réseau de l'URCA votre machine au moins tous les six mois pour qu'elle se remette à jour et que vous ne courriez pas de risques en termes de sécurité,
- A ne pas désinstaller les outils d'administration mis en place par l'informatique de proximité de l'URCA,
- A faire appel à l'informatique de proximité, si l'ordinateur est réinstallé par l'utilisateur,
- A ne pas modifier et/ou supprimer le compte administrateur sur l'ordinateur qu'il a reçu de la part de l'URCA,
- A informer le service informatique de proximité, pour tout ordinateur commandé sur les crédits de l'URCA et qui doit être intégré dans l'annuaire Active Directory géré par la DN.

Vous devenez garant du bon fonctionnement de l'ordinateur au même titre que la DN. Il est de votre responsabilité de sauvegarder vos données régulièrement car, étant ponctuellement administrateur, toute manipulation hasardeuse pourra avoir des conséquences dommageables.

Article XIV. Statut de la charte

Le non-respect de la charte est susceptible d'engager la responsabilité professionnelle de l'Administrateur et peut aboutir à des sanctions disciplinaires définies par le règlement intérieur.

Par ailleurs, l'Administrateur engage pleinement sa responsabilité en cas d'infraction ou de complicité à la législation ou à la réglementation en vigueur.

- Les principales dispositions légales en vigueur prévues par la législation française et la réglementation européenne dans le domaine de la sécurité des Systèmes d'Information sont notamment les suivantes :
- La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD),
- La législation relative à la fraude informatique (articles 323-1à 323-7 du Code pénal),
- La législation relative à la propriété intellectuelle,
- La loi du 04/08/94 relative à l'emploi de la langue française,
- La législation applicable en matière de cryptologie,
- La législation en matière de transmission d'informations à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine et la diffusion de contenus illicites à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste et sexiste (articles 227-23 et 227-24 du Code pénal et loi du 29 juillet 1881)

Annexe 3

Charte régissant l'usage du système d'information au sein de l'Université de Reims Champagne-Ardenne

SOMMAIRE

Préambule

La présente charte a pour objet de fixer les règles d'usage des moyens numériques de l'Université de Reims Champagne-Ardenne (URCA).

Par l'expression « moyens numériques », la présente charte vise tous les éléments ou toutes les ressources constituant le système d'information de l'URCA.
Ainsi, les moyens numériques représentent l'ensemble des logiciels et matériels, outils informatiques et services numériques, que l'URCA met à disposition de ses utilisateurs.

Les « **utilisateurs** », au sens de la présente charte, sont définis comme l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'URCA.

Ainsi sont notamment désignées :
Tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche,
Tout étudiant inscrit dans l'un des établissements de l'URCA,
Tout prestataire ou partenaire ayant contracté avec l'URCA,
Toute personne autorisée à accéder à un service numérique.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte a pour objet de fixer les règles d'usage des moyens numériques de l'URCA.

Ces règles ont pour but de contribuer à la sécurité du système d'information et de garantir l'intégrité et la confidentialité des données qui y sont hébergées.

L'usage raisonné des moyens numériques concourt par ailleurs à une conciliation saine et équilibrée des temps de vie professionnel et personnel.

Engagements de l'URCA
L'URCA porte à la connaissance de l'utilisateur la présente charte.

L'URCA met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'URCA facilite l'accès des utilisateurs aux ressources du système d'information nécessaires. Les ressources mises à leur disposition sont prioritairement à usage universitaire mais l'établissement est tenu de respecter la vie privée de chacun dans les conditions décrites section II-1.

Engagements de l'utilisateur
L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

Les utilisateurs sont responsables de l'utilisation qu'ils font des ressources mises à leur disposition par l'URCA.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat. L'utilisateur dans son utilisation est soumis au droit français et communautaire.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'institution ainsi qu'à l'ensemble des utilisateurs.

Les dispositions de la présente charte s'appliquent également aux utilisateurs membres du personnel de l'URCA autorisés à exercer leurs missions dans les conditions de télétravail.

Les utilisateurs ayant des fonctions d'administrateur des moyens numériques seront soumis à une charte complémentaire et spécifique précisant leurs obligations particulières.

Article II. Conditions d'utilisation des systèmes d'information

Section II.1 Utilisation professionnelle / privée

L'URCA met à la disposition de ses utilisateurs un ensemble d'outils et de services numériques à des fins professionnelles.

Au sens de la présente charte, l'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :
Dans le cadre des missions confiées par l'URCA, pour les utilisateurs membres de son personnel : enseignants, personnels administratifs ou techniques, mais également ses prestataires et partenaires,
Dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.

Les personnels s'engagent à utiliser les applications numériques fournies par l'Université si celles-ci fournissent les mêmes services qu'un outil externe qui pourrait collecter des informations sensibles.

Par opposition, l'utilisation à des fins privées doit être non lucrative et limitée, tant dans la fréquence que dans la durée. Elle ne doit nuire ni à la qualité du travail de l'utilisateur, ni au temps qu'il y consacre, ni au bon fonctionnement du service, et sous réserve du respect de la politique de sécurité et des obligations de loyauté et de confidentialité.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu à cet effet et identifié sans ambiguïté comme tel. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

Ainsi, tout utilisateur manifestera le caractère extra-professionnel d'une partie de ses données en adoptant, exclusivement, les termes « **privé** », « **personnel** » ou « **confidentiel** », pour nommer le dossier ou l'objet du message contenant ces informations.

Concernant les réseaux sociaux, les utilisateurs se doivent d'adopter un comportement en lien avec leurs fonctions, vis-à-vis de leurs employeurs lors de l'utilisation des réseaux sociaux, des blogs, qu'ils soient professionnels ou non professionnels.

Section II.2 Matériel personnel / professionnel

L'usage de ressource informatique personnelle (un ordinateur, une tablette, un smartphone, un objet connecté, une clé USB, …) acheté sur des crédits personnels, lorsqu'elles sont utilisées pour accéder au système d'information de l'URCA, ne doit pas remettre en cause ou affaiblir la sécurité en vigueur dans l'établissement. Lorsque des données professionnelles (propriété de l'URCA) sont présentes sur des ressources informatiques personnelles, il incombe à l'utilisateur de mettre tout en œuvre pour protéger ses données.

Le personnel disposant de ressource informatique et/ou audiovisuelle professionnelle (un ordinateur, une tablette, un smartphone, un objet connecté, une clé USB, connectique, vidéoprojecteur, …) fourni par l'établissement, la composante, le laboratoire, ..., accepte la politique de gestion de ses ressources mise en place par l'URCA. A la fin de la mission lui ayant value mise à disposition du matériel, l'utilisateur s'engage à le restituer à l'établissement.

Section II.3 Outils de communication / Cloud computing

L'évolution des outils de communication sous différentes formes (réseaux sociaux, forums, espaces de contribution, messageries instantanées, …) et utilisés dans un cadre personnel sont autorisés à la condition d'un usage raisonnable et raisonné. L'utilisation de ces différents outils dans un cadre personnel et/ou professionnel doivent rester cordiaux.
Il est à rappeler auprès de tous les utilisateurs de l'URCA leur responsabilité, ainsi que leurs obligations attenant à leur statut, même en cas de publications réalisées en dehors du temps de travail.

Dès lors que l'université met à disposition des moyens numériques, il convient de préciser que la responsabilité de l'URCA peut être engagée eu égard aux agissements de ses utilisateurs sur les outils de communication.

L'usage de service de « *Cloud computing* » (informatique dans les nuages) externes à l'URCA est toléré. Toutefois, il est primordial que les données sensibles (données de recherche, données administrative, …) du système d'information ne sortent pas du périmètre maîtrisé par l'URCA.

Section II.4 Continuité de service : gestion des absences et des départs

Afin d'assurer la continuité de service, l'utilisateur doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe.

Concernant les données professionnelles : il appartient au chef de service de l'utilisateur de s'assurer qu'il a accès aux données professionnelles nécessaire à la continuité de service et d'autoriser expressément, le cas échéant, toute copie totale ou partielle de ces données par l'utilisateur avant son départ. Cette autorisation est remise à l'utilisateur.

Les étudiants pourront encore consulter pendant six mois après la fin de leur inscription dans l'établissement. La procédure de fermeture s'engagera quelques temps après ces six mois.
Les personnels conservent un accès au bureau virtuel de l'URCA pendant trois mois et à la messagerie de l'URCA pendant un an à l'issue de leur fin de contrat. Il est de la responsabilité du personnel de récupérer ses données avant son départ.
Les doctorants relèvent des règles relatives aux personnels dans la présente charte.

En tout état de cause les données non situées dans les répertoires « **privé** », « **personnel** » ou « **confidentiel** », sont considérées comme des données appartenant à l'établissement qui pourra en disposer.

Section II.5 Droit à la déconnexion et l'usage des emails à l'URCA

Le développement du numérique favorise de nouvelles formes de travail et brouille la limite entre vie personnelle et vie professionnelle. Dans ce contexte, il apparaît important de rappeler un certain nombre de recommandations qui doivent s'appliquer à l'ensemble des membres de la communauté universitaire :

Tous les personnels, quels que soient leur grade, leur statut ou leur emploi sont invités à adopter une attitude raisonnée et éthique dans l'utilisation de la messagerie professionnelle, qui respecte les personnes et leur vie privée,
L'usage de la messagerie doit être approprié et ne peut se substituer au dialogue ou aux échanges entre les personnes. Ce dialogue et ces échanges contribuent au lien social,
L'usage de la messagerie doit se faire dans le respect des règles de courtoisie et de politesse,
L'envoi de messages électroniques est à éviter (sauf urgence) en dehors des horaires habituels de travail, soit entre 19h et 8h, le week-end et les jours fériés,
Les personnels ne sont pas tenus de répondre aux messages électroniques en dehors des horaires habituels de travail, pour préserver au mieux la distinction entre vie privée et vie professionnelle.

Article III. Principes de sécurité

Section III.1 Règles de sécurité applicables

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

L'utilisateur est informé que 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 garder strictement confidentiels son (ou ses) codes 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,
De respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe.

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

Veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de continuité du service mises en place par la hiérarchie (Cf. section II.2),
Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

de la part de l'utilisateur :
De verrouiller son poste de travail en cas d'absence et d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail,
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,
Ne pas installer, télécharger ou utiliser sur le matériel de l'URCA, des logiciels ou progiciels sans respecter les droits de licence; les logiciels doivent être utilisés dans les conditions des licences souscrites,
Se conformer aux dispositifs mis en place par les établissements pour lutter contre les virus et les attaques par programmes informatiques,
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.

Devoirs de signalement et d'information
L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, suspicion d'une usurpation d'un code d'accès, il signale également à son responsable toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation. L'utilisateur ou sa hiérarchie informera les RSSI (Responsables de la Sécurité des Systèmes d'Information) de l'établissement concerné à l'adresse de contact rssi@univ-reims.fr

Section III.2 Mesures de contrôle de la sécurité

L'utilisateur est informé :
Que pour effectuer la maintenance corrective, curative ou évolutive, l'URCA se réserve la possibilité de réaliser des interventions (le plus souvent à distance) sur les ressources matérielles et logicielles mises à sa disposition,
Qu'une maintenance à distance est précédée d'une information de l'utilisateur,
Que toute situation bloquante pour le système ou générant une difficulté technique, pourra conduire à l'isolement du poste voire à la suppression des éléments en cause,

Que les outils du système d'information dont la conformité au RGPD et l'information aux personnes concernées ont été effectuées peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire, de suivi fonctionnel, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable,
Qu'il lui est formellement interdit de désinstaller les outils d'administration mis en place par l'informatique de proximité de l'URCA,
Que si l'ordinateur est réinstallé par l'utilisateur, il doit faire appel à l'informatique de proximité pour l'accompagner dans cette démarche,
Qu'il lui est interdit de modifier et/ou supprimer le compte administrateur sur l'ordinateur qu'il a reçu de la part de l'URCA,
Tout ordinateur commandé sur les crédits de l'URCA devrait être intégré dans le système d'authentification de l'URCA Les personnels chargés du bon fonctionnement des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Section III.3 Protection antivirale

L'URCA a déployé une protection logicielle généralisée non seulement sur les serveurs mais aussi les postes de travail des utilisateurs.
Le but d'un anti-virus est de protéger toutes les machines du parc contre les attaques provoquées par des codes malveillants. Sur chaque poste utilisateur est installé un client anti-virus. Il est interdit par la présente charte de désactiver, d'altérer le fonctionnement ou de désinstaller ce client. Il est aussi interdit d'utiliser d'autres logiciels (anti-virus ou autres) susceptibles d'entraîner un dysfonctionnement de l'anti-virus installé en exécution de la stratégie de sécurité de l'URCA. L'URCA ayant souscrit dans le cadre d'un marché national pour la fourniture d'antivirus, il est formellement interdit d'utiliser un autre antivirus ne relevant pas de ce marché sur un poste de l'université.

Article IV. Communication électronique

Section IV.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'URCA.
La messagerie est un outil de travail destiné à des usages professionnels : elle peut constituer le support d'une communication privée telle que définie à la section II.1.

(a) Adresses électroniques

L'URCA s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

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.

Des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'« utilisateurs », pourront être mises en place par l'URCA.

Certaines listes institutionnelles sont utilisées au sein de l'établissement et ne peuvent donner lieu à un désabonnement de la part de l'utilisateur.

(b) Contenu des messages électroniques

Par référence à l'article II, section II.1, tout message sera réputé professionnel sauf s'il comporte en objet la mention « **privé** », « **personnel** » ou « **confidentiel** », ou s'il est stocké dans un espace spécifique de données identifié comme tel.

Pour préserver le bon fonctionnement des services, des limitations pourront être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus, …) seront déployées.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature.
Les auteurs de messages contenant de telles mentions sont susceptibles de faire l'objet de poursuites pénales

ainsi que de poursuites disciplinaires par l'établissement.

(c) 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. Des recommandations sont présentées dans le guide pratique de l'utilisateur annexé à la présente charte.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent juridiquement former un contrat, sous réserve du respect des conditions fixées par les articles 1101 et suivants du code civil.

L'utilisateur doit, en conséquence, être vigilant sur le contenu des messages électroniques qu'il échange à l'instar des courriers traditionnels.

En application du Code des relations entre le public et l'administration que désormais les échanges électroniques entre l'administration et un usager/un de ses agents peuvent valoir décision administrative.
Les échanges électroniques de ce type doivent par conséquent se conformer aux exigences en vigueur pour ce genre d'actes administratifs.

Un courriel peut engager administrativement l'établissement.

(e) Stockage et archivage des messages

Chaque utilisateur doit organiser et assurer la conservation des messages pouvant être indispensables à l'exercice de ses activités ou simplement utiles en tant qu'éléments de preuve.

Le guide pratique de l'utilisateur, annexé à la présente charte, présente un ensemble de règles impératives et de recommandations dont le respect garantit la conservation de ces données.

(f) Gestion des absences

En cas d'absence de l'utilisateur, celui-ci s'engage à utiliser tant que possible le gestionnaire d'absence de l'outil de messagerie qui permet de renseigner le texte de la réponse automatiquement adressée à chaque expéditeur en précisant en particulier la période d'absence et les autres adresses où le message peut être envoyé en cas de nécessité.

Lors de la mutation d'un « utilisateur », il convient d'éviter que sa boîte de messagerie continue à recevoir des messages au titre des fonctions qu'il quitte.
En cas de départ définitif de l'institution pour éviter que des courriers électroniques ne soient pas relevés, que des boites de messagerie demeurent inutilisées, que des messages personnels ou confidentiels soient lus par des agents qui ne sont pas destinataires, l'utilisateur s'engage à suivre la procédure suivante :
L'utilisateur envoie un message à ses correspondants habituels leur indiquant la date de son départ et leur signalant la boîte de messagerie à laquelle ils devront envoyer leurs messages à partir de cette date au titre des fonctions qu'il quitte (adresse de messagerie de son successeur s'il est connu, boîte de l'intérimaire ou boîte fonctionnelle),
Juste avant son départ, l'utilisateur archive dans un fichier les messages qu'il doit transmettre à son successeur et remet ce fichier à son supérieur hiérarchique,
L'utilisateur s'engage à ré-aiguiller les messages qu'il reçoit durant la période où la messagerie reste active après son départ et qui sont destinés à son ancien service.

En cas de décès de l'utilisateur ou s'il s'absente sans préavis et est injoignable, l'institution se réserve le droit de supprimer tout message de réponse automatique ou de redirection qui impacterait le bon fonctionnement des services. Un autre message de réponse automatique pourra être rajouté en tant que de besoin à la discrétion de l'institution. Le service en charge de la messagerie, sur demande écrite du (de la) président(e) et selon les modalités définies à l'article (g), pourra accéder à la boîte de messagerie afin de transmettre les messages nécessaires à la continuité de service. C'est pourquoi il est recommandé d'utiliser les adresses de messagerie fonctionnelles plutôt que nominatives.

(g) Décès ou départ soudain de l'utilisateur

Dans le cas du décès ou d'un départ de l'utilisateur et notamment pour les besoins de la continuité de service, l'institution pourra être amenée à supprimer tout message de réponse automatique qui aurait été rédigé et à mettre en place un nouveau message indiquant vers qui les expéditeurs doivent se tourner. Si une redirection des messages électroniques était en place, cette dernière pourra également être supprimée. De plus, le compte de messagerie est verrouillé ainsi que les accès aux services numériques à partir du compte de cette personne, 24 heures maximum après la saisie de l'information du décès ou du départ dans la base de données des ressources humaines ou de la scolarité par les services habilités. Les données de l'utilisateur sont cependant conservées afin de pouvoir être fournies en cas de réquisition judiciaire ou sur demande du (de la) Président(e) de l'institution pour assurer la continuité de service.
En cas de décès, la famille ne peut demander sans décision de justice la récupération des données.

(h) Modalités d'accès à une boîte de messagerie

Sur demande du (de la) Président(e) de l'institution et en cas d'absence prolongée ou de décès d'un personnel, en invoquant la continuité de service pour justifier la transmission de certains messages, dans ce cas, l'accès à la messagerie est strictement encadré avec la présence de témoins (le RSSI et le DPO) qui garantissent la procédure. Les messages dont le sujet comporte « **privé** », « **confidentiel** » ou « **personnel** » ou dont l'objet est sans rapport avec la demande de continuité de service ne peuvent être accédés.

Section IV.2 Internet

Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur.

L'utilisation de la technologie 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'URCA.

L'URCA met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail destiné à des usages professionnels : il peut constituer le support d'une communication privée telle que définie en section II.1, dans le respect de la règlementation en vigueur.

Il est rappelé que la consultation volontaire de contenus à caractère illicite (notamment pédopornographique, raciste, xénophobe, incitation à la violence, …) est proscrite.
Les utilisateurs sont informés qu'en considération de la mission éducative de l'établissement, la consultation volontaire et répétée de contenus à caractère pornographique depuis les locaux de l'URCA est proscrite, sauf en cas de travaux de recherches scientifiques sur ce sujet.

Section IV.3 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de propriété intellectuelle tels que définis à l'article VI.

L'URCA 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, tels les virus, code malveillant ou programmes espions.

Section IV.4 Anti-Plagiat

La mise à disposition d'un outil de détection de similitude ou anti-plagiat, s'inscrit dans une perspective non répressive et d'aide à la prise de décision.
Par conséquent, cet outil et les indicateurs fournis, ne peuvent fonder à eux seuls une décision de sanction.

L'accès à l'outil est activé par le Service des Usages du Numérique, après une prise de contact avec l'un des référents anti-plagiat ou la participation à une formation spécifique.

Cet outil ne concerne que les travaux des étudiants ou stagiaires et uniquement dans le contexte de l'enseignement.

Section IV.5 Respect des clauses contractuelles

L'usage des ressources documentaires électroniques éditoriales doit respecter les conditions contractuelles

des licences souscrites par l'université.

D'une façon générale, et sauf mention contraire explicite dans la licence, indiquée clairement sur le site de la bibliothèque, les éditeurs n'autorisent qu'une utilisation « raisonnable » et personnelle des ressources documentaires électroniques, dans un but strictement non-commercial et à des fins pédagogiques ou de recherche.
Les termes ci-dessus doivent être entendus de la manière suivante :
Utilisation raisonnable : L'utilisateur s'engage à ne pas télécharger de livres complets (hors livres numériques proposés en tant qu'entités téléchargeables sur des plateformes dédiées, ou sur des liseuses ou tablettes de lecture prêtées par la bibliothèque) ou de fascicules entiers de revues, ainsi qu'à ne pas utiliser d'aspirateur de site web.
Utilisation personnelle : L'utilisateur s'engage à faire un usage personnel des ressources électroniques documentaires : aucune diffusion à une personne extérieure à l'université, même à titre gratuit, n'est autorisée, ni sous forme de copies imprimées, ni sous forme électronique.
Utilisation dans un cadre pédagogique ou de recherche : L'utilisateur s'engage à n'utiliser les ressources documentaires électroniques que dans le cadre strict de ses études, de son enseignement ou de sa recherche.

Aucune utilisation à des fins commerciales n'est autorisée. Les documents ou les données ainsi que leur exploitation ne peuvent pas être destinés à une entreprise dans laquelle un étudiant serait en stage, ou être utilisés par un enseignant ou un étudiant dans le cadre d'une activité professionnelle pour le compte d'un cabinet ou d'une entreprise.

Article V. Traçabilité

Cette traçabilité est mise en place conformément au RGPD et à la loi du 6 janvier 1978 modifiée.

Les utilisateurs sont informés que la durée légale de conservation des fichiers de journalisation est d'une année à partir de la date d'enregistrement.

Article VI. Confidentialité

Chaque « utilisateur » a une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel auxquels il a accès dans le système d'information. Le respect de cette confidentialité implique notamment :
De veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations,
De respecter les règles d'éthique professionnelle et de déontologie, ainsi que l'obligation de réserve et le devoir de discrétion.

Article VII. Respect de la propriété intellectuelle

L'URCA rappelle que l'utilisation des moyens numériques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :
Utiliser les logiciels dans le strict respect des licences souscrites,
S'abstenir de 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 autre droit privatif, sans avoir obtenu préalablement l'autorisation du ou des titulaires de ces droits.

Article VIII. Respect du cadre réglementaire Informatique et Libertés

L'utilisateur est informé de la nécessité de respecter le Règlement Général sur la Protection des Données (règlement UE 2016/676 dit RGPD) et la loi du 6 janvier 1978 modifiée (loi Informatique et Libertés).

Les données à caractère personnel sont des informations qui permettent l'identification des personnes physiques auxquelles elles se rapportent, directement ou indirectement, et à partir d'une seule donnée ou à partir du croisement d'un ensemble de données.

Toutes les créations ou modifications de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la réglementation en vigueur.

En conséquence, tout utilisateur souhaitant procéder à une telle création ou modification de fichiers devra préalablement contacter le DPO (Délégué à la Protection des Données) de l'URCA à l'adresse suivante : dpo@univ-reims.fr

L'utilisateur a l'obligation d'alerter le DPO et le RSSI en cas de violation de données à caractère personnel.

De plus, conformément aux dispositions du Règlement Général sur la Protection des Données (RGPD) et à la loi du 6 janvier 1978 modifiée, chaque utilisateur dispose d'un droit d'accès, de rectification et d'effacement ainsi que d'un droit d'opposition, d'un droit à la limitation du traitement et d'un droit à la portabilité relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information.

Article IX. Limitation des usages

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extraprofessionnelles, est passible de sanctions disciplinaires et pénales.

Article X. Entrée en vigueur de la charte

La présente charte sera intégrée au règlement intérieur de l'URCA.

La présente charte s'ajoute à tous les autres documents ou chartes.

Est annexé à cette charte les documents suivants :
guide d'utilisation,
annexe juridique.

Approuvée par le conseil d'administration du 19/10/2021

Annexe 4
Approuvée par le conseil d'administration le 12 décembre 2023

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION (PSSI)

PSSI-Générale

Université de Reims Champagne-Ardenne

Référence : PSSI-G URCA V1

Responsable du projet : RSSI	EMAIL :	rssi@univ-reims.fr
Version : Date : 22/11/2023	1.0	Création du document

SOMMAIRE

1. Préambule

1.1. Objectif du document

Ce document constitue la Politique de Sécurité des Systèmes d'Information Générale (PSSI-G) de l'Université de Reims Champagne-Ardenne (URCA). Il fixe les objectifs, l'organisation en matière de sécurité et les principes de sécurité applicables de façon transverse à tous les systèmes d'information de l'URCA.

Cette politique générale est rédigée et maintenue à jour par le Responsable de la Sécurité des Systèmes d'Information (RSSI). Elle s'appuie sur les orientations stratégiques de la direction générale ainsi que sur des normes et réglementations nationales et internationales sur la sécurisation des Systèmes d'Information.
La PSSI-G fait partie intégrante du référentiel cybersécurité de l'URCA.

1.2. Périmètre d'application

La PSSI-G s'applique de façon transverse à toutes les directions et tous les systèmes d'information de l'URCA.

1.3. Évolution

La présente PSSI-G doit évoluer pour tenir compte des changements qui peuvent affecter les systèmes d'information et l'environnement, notamment en termes d'enjeux et de menaces. Elle doit en conséquence être mise à jour en fonction :

- Des évolutions de la réglementation et des engagements contractuels avec les partenaires ;
- Des évolutions des exigences issues de l'autorité de tutelle (le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation) ;
- Des nouvelles menaces et risques liés à l'évolution des technologies des systèmes d'information et à leur complexification ;
- Des évolutions des systèmes d'information ;
- Des résultats des audits concernant sa mise en application ;
- Des conclusions tirées des rapports de traitement des incidents.

La révision de la PSSI-G est réalisée, au minimum une fois tous les 3 ans, par le RSSI puis proposée à la Direction Générale de l'établissement pour validation.

1.4. Diffusion

La politique de Sécurité Générale est un document interne de l'URCA. Il est

communiqué aux agents publics, à l'autorité de tutelle et aux partenaires, lorsque c'est nécessaire et dès lors qu'ils sont acteurs des systèmes d'information.
Elle peut également être communiquée par le RSSI au cas par cas et sur demande écrite et justifiée à d'autres tiers extérieurs (exemple : organisations officielles, laboratoires, écoles ou universités partenaires, auditeurs externes, prestataires, etc.).

1.5. Entrée en vigueur

La politique de sécurité est validée par la direction générale. Elle entre en vigueur dès diffusion à l'ensemble des agents publics.

Toutes les directions de l'URCA doivent respecter les principes fondamentaux édictés dans cette politique générale ainsi que dans les différentes politiques de sécurité opérationnelles associées. Elles doivent également être contractuellement imposées aux partenaires et prestataires de l'URCA.

2. Enjeux et objectifs de la sécurité de l'URCA

2.1. Les enjeux en matière de sécurité

2.1.1. Sécuriser les SI : une nécessité

L'évolution sans cesse croissante des technologies et des systèmes de traitement de l'information et celle, concomitante, des menaces informatiques et des cyberattaques, justifie l'attention que l'URCA porte à la sécurité de ses systèmes d'information.

Cette attention porte sur la protection des systèmes d'information critiques, mais aussi plus largement sur la protection du patrimoine informatique de l'URCA qui constitue un actif clé.

De manière accidentelle ou délibérée, provenant de l'interne ou de l'externe, dans un cadre ciblé ou opportuniste, un incident de sécurité pourrait entraîner des conséquences sérieuses pour l'URCA et pour ses partenaires (industriels, ministères, écoles, laboratoires de recherche, etc.) :

- Perte du patrimoine informationnel, par la destruction massive de données de recherche, de formation, de scolarité, se traduisant par une perte de valeurs et/ou désorganisant durablement l'établissement ;
- Arrêt ou dysfonctionnement de certains processus de l'établissement à des périodes critique, empêchant la création des dossiers de scolarisation des étudiants voire l'indisponibilité complète des processus de formation et de scolarité (plus de diplomation possible) ;

- Divulgation de données sensibles valorisables (propriété industrielle, innovation scientifique : fuite du secret industriel des partenaires (informations sensibles reçues dans le cadre de partenariat de recherche), fuite de données de santé traitées par la recherche, fuite des données personnelles des étudiants ou des agents publics ;
- Attaque d'un partenaire au travers de l'établissement, de ses SI ou de son personnel ;
- Atteinte à l'intégrité sur les résultats de scolarité pour un ou plusieurs étudiants ;
- Atteinte à l'image en qu'université formant aux Réseaux et Télécommunications, avec une composante cybersécurité ;
- Risque juridique, par exemple amende infligée par la CNIL en raison d'une négligence ayant mené à l'exfiltration de données personnelles protégées par la loi, ou liées à une violation de propriété intellectuelle.

Il est donc nécessaire de protéger et de sécuriser les systèmes d'information de l'URCA, et ce à la hauteur des enjeux qu'ils représentent et en cohérence avec les risques et les menaces qui pèsent sur eux.

2.1.2. Sécuriser les SI : une obligation

Sécuriser les systèmes d'information de l'URCA est également une obligation pour s'aligner avec les évolutions du cadre légal, réglementaire et contractuel (hors droit européen et français).

Le RSSI peut, lorsqu'il le juge nécessaire, s'appuyer sur la Direction des Affaires Juridiques pour accomplir sa mission.

2.1.3. Sécuriser les SI : une opportunité

La sécurité des systèmes d'information est également appréhendée par l'URCA comme une opportunité lui permettant, d'une part, d'adopter sereinement les avancées technologiques, et d'autre part de renforcer la relation de confiance avec ses partenaires (industriels, universitaires, laboratoires, etc.) et le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation.

Lorsque la sécurité est traitée en amont des projets, précisément gérée par des acteurs identifiés et avec l'engagement de la Direction, son coût peut être rationalisé et son retour sur investissement, certes indirect, peut être maximisé.

Le RSSI de l'URCA veille à la prise en compte de la présente PSSI-G dans les projets de systèmes d'information, en faisant mener les analyses de risques nécessaires, en

décidant des mesures de sécurité techniques ou organisationnelles à mettre en place et en contrôlant leur application.

2.2. Les objectifs stratégiques en matière de sécurité

Afin de répondre aux enjeux de sécurité précédents, l'URCA a défini des objectifs stratégiques qui constituent la cible à atteindre en matière de sécurité des systèmes d'information :

- Permettre aux différentes directions d'assurer, même de façon dégradée, les activités métiers ;
- Être en mesure d'anticiper et de contribuer à la gestion coordonnée des situations de crise relatives aux systèmes d'information et celles susceptibles d'interrompre les activités de l'URCA ou de nuire à son image ;
- Respecter les exigences réglementaires et législatives auxquelles sont assujetties les différentes directions de l'URCA ;
- Ne pas compromettre les données des partenaires, les données de santé fournies ou l'écosystème qui gravite autour de l'URCA ;
- Protéger son personnel, ses actifs, ses partenaires et ses étudiants contre toute forme de menace, accidentelle ou intentionnelle ;
- Contribuer à la performance globale de l'URCA et préserver sa réputation et son image en tant qu'université formant notamment à la cybersécurité ;
- Faire de la sécurité un facteur d'opportunité et de croissance dans la création de nouveaux systèmes, notamment en anticipant les évolutions (nouvelles menaces, nouvelles technologies …) et en répondant aux attentes des directions, du ministère et des partenaires.

Afin de satisfaire ses objectifs stratégiques, l'URCA définit un ensemble de politiques de sécurité opérationnelle qui propose des règles et des mesures techniques. Ces politiques opérationnelles visent à garantir une protection efficace, rationalisée, proportionnée aux enjeux et améliorée dans le temps des activités et des processus de l'URCA.

Les politiques de sécurité opérationnelle sont élaborées sur la base des fonctions de sécurité ci-dessous :

- **L'Anticipation** : Anticiper l'occurrence de menaces et de toute non-conformité réglementaire (Gestion des risques, Gestion de la conformité réglementaire, Gestion de la conformité avec les exigences contractuelles des partenaires, etc.) ;

- **La Protection** : Mettre en place des mécanismes de protection adaptés (Protection des actifs, Protection des biens supports, Protection des informations reçues de la part des partenaires, etc.) ;
- **La Détection** : Détecter les événements de sécurité pour se donner la capacité de réagir (Journalisation, Corrélation, Détection, etc.) ;
- **La Réaction** : Réagir face à des incidents de sécurité et reconstruire les actifs pour assurer une reprise d'activité dans les plus brefs délais (Gestion des incidents, Reprise d'activité, Retour à la normale, etc.) ;
- **L'Amélioration** : S'inscrire dans une logique d'adaptation dynamique des postures de sécurité et d'amélioration continue.

Le respect des politiques de sécurité opérationnelle est une obligation de tous les acteurs - interne et externe – de l'URCA, en lien direct ou indirect avec les systèmes d'information.

3. Le référentiel cybersécurité de l'URCA

Le référentiel cybersécurité de l'URCA est composé de trois niveaux :

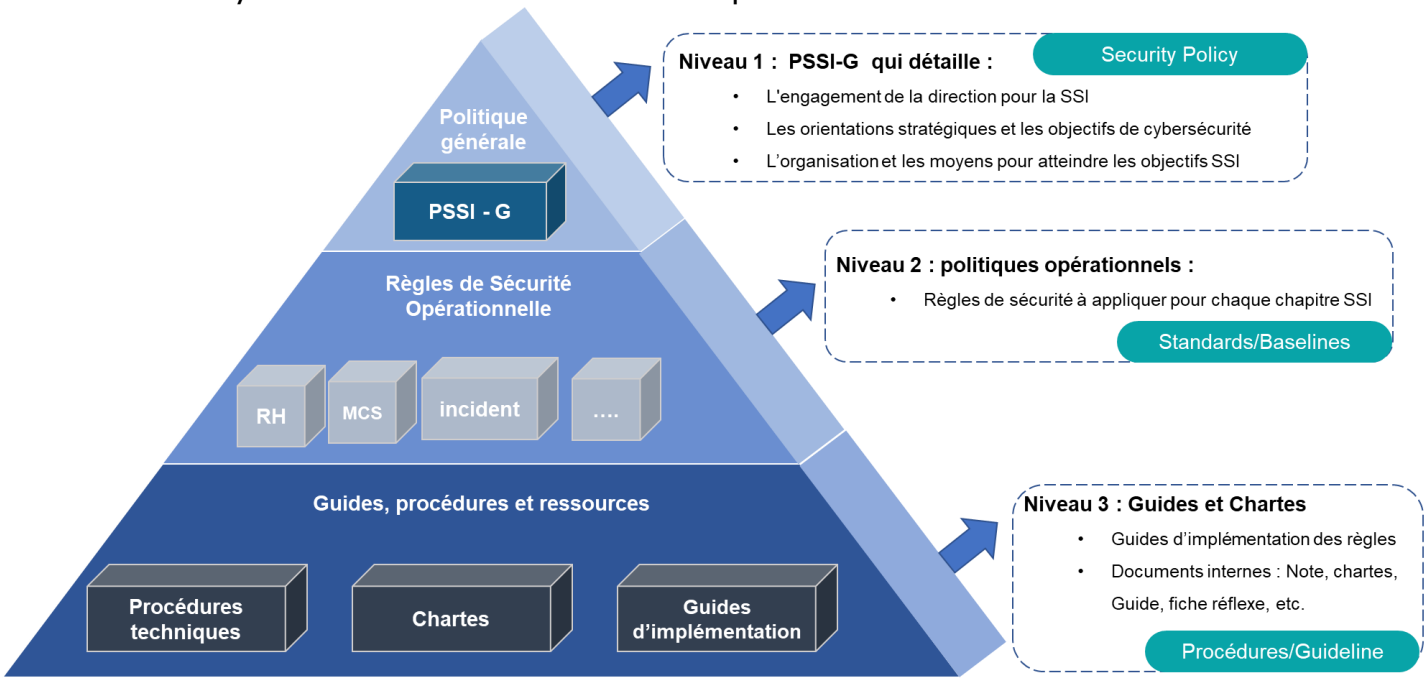


Figure 1 : Eléments constitutifs du référentiel cybersécurité

- **Niveau 1** : Définit la Politique de Sécurité des Systèmes d'information Générale applicable de façon transverse à l'ensemble des systèmes d'information de l'URCA (le présent document) ;
- **Niveau 2** : Définit les déclinaisons opérationnelles des objectifs stratégiques de l'URCA. Cette politique opérationnelle (PSSI-Opérationnelle) formalise les

règles de sécurité applicables pour l'ensemble des systèmes d'information de l'URCA afin d'atteindre les objectifs stratégiques ;

- **Niveau 3** : Définit les guides et les méthodes proposées pour un déploiement correct et cohérent des règles de sécurité.

Ces politiques et procédures de sécurité sont issues d'une analyse des risques cybersécurité réalisée et régulièrement mise à jour par le Responsable de Sécurité des Systèmes d'Information.
Elles constituent le cadre de référence conçu pour atteindre les objectifs en matière de sécurité des SI. Elles traduisent la feuille de route que l'URCA entend suivre et faire prendre en compte par toutes les parties prenantes afin d'atteindre la cible définie en matière de sécurité.

4. Organisation et Management de la sécurité des SI

4.1. Rôles en matière de sécurité

4.1.1. Président (Autorité Qualifié SSI)

La maîtrise et la gestion de la sécurité globale relèvent de la responsabilité première du Président (en sa qualité d'AQSSI) de l'URCA. Il porte ainsi la responsabilité de la gestion des risques cybersécurité et des travaux de mise en conformité réglementaire.

Cette responsabilité lui incombe de se doter des moyens et de l'organisation les plus adaptés pour gérer les risques et la conformité réglementaire relatifs aux systèmes d'information de l'URCA. À ce titre, le Président réalise, sur la base des travaux effectués par le RSSI, un arbitrage sur l'acceptation des risques et sur la conformité réglementaire et contractuelle, et décide les budgets et les moyens mis à disposition pour le programme sécurité.

La direction générale exprime son leadership et son engagement en faveur du programme sécurité de l'URCA en :

- S'assurant que la politique et les objectifs sécurité sont établies et qu'ils sont compatibles avec l'orientation stratégique de l'URCA ;
- S'assurant que les ressources nécessaires pour la mise en place du plan d'action sont disponibles ;
- Communicant sur l'importance d'une continuité d'activité efficace et de se conformer aux exigences de la politique de sécurité ;

- S'assurant que la politique de sécurité atteint les résultats et objectifs escomptés ;
- Orientant et soutenant les membres de l'URCA pour qu'elles contribuent à l'efficacité du plan d'action et qu'elles respectent les règles de la politique de sécurité ;
- Promouvant l'amélioration continue ;
- Aidant les autres directeurs et responsables concernés à démontrer leur leadership et leur engagement dès lors que cela s'applique à leurs domaines de responsabilité.

4.1.2. Responsable de la Sécurité des Systèmes d'Information

Le RSSI a la responsabilité, au sein de la Direction du Numérique (DN), de conseiller et d'accompagner la Direction Générale dans la définition d'un programme sécurité, conformément aux risques identifiés, aux obligations légales et contractuelles et aux objectifs stratégiques, d'en contrôler le respect et d'exercer un reporting pour assurer le suivi au plus haut niveau du programme.

Cette responsabilité se décline en mission d'expertise, de pilotage et de support :

- Concevoir la gouvernance et le cadre de référence de la sécurité (Politiques et Procédures de sécurité) et veiller à son déploiement ainsi qu'à sa bonne application au sein de toutes les directions de l'URCA ;
- Identifier et fournir la visibilité sur les risques / impacts majeurs ainsi que sur l'efficacité des capacités mises en œuvre pour les traiter ;
- Constituer un pôle d'expertise à même d'assister et de conseiller les directions sur les nouveaux usages et risques sécurité sur leur périmètre d'activité et projet, pour leur permettre de répondre aux enjeux métiers en réalisant des analyses de risques, en proposant des mesures de sécurité pour traiter les risques identifiés et en contrôlant la bonne application des mesures de sécurité ;
- S'assurer de la correcte mise en œuvre des règles de la politique de sécurité, et de la prise en compte des aspects sécurité dans les actions et les projets menés au sein de chaque direction de l'URCA ;
- Contribuer au suivi et à la gestion des incidents de sécurité de l'URCA ;
- Gérer les évolutions des Politiques de Sécurité des Systèmes d'Information et de l'analyse des risques ;

- Participer à la sensibilisation et la formation des agents publics de l'URCA à la sécurité des SI ;
- Assurer le reporting vis-à-vis de la direction générale.

4.1.3. Délégué à la protection des données (DPO)

La DPO a la responsabilité de conseiller et d'accompagner la Direction Générale dans la définition d'un programme de mise en conformité avec les exigences juridiques, techniques et sécurité du RGPD.

Le DPO a la responsabilité de contrôler le respect du programme de mise en conformité et d'exercer un reporting pour assurer le suivi au plus haut niveau du programme.

En particulier, le DPO a la responsabilité de traiter, avec l'appui de la DN et du RSSI, d'identifier les incidents RGPD se produisant sur le SI, et de contrôler l'application du plan de traitement des risques identifiés.

4.1.4. Responsables

Chaque directeur de recherche, directeur d'unité et chaque responsable des services, d'UFR, instituts et écoles a la responsabilité, au sein de son équipe, de sensibiliser les agents publics sur la nécessité de respecter les règles de la politique de sécurité des systèmes d'information.

Cette responsabilité se décline en mission d'appui et de support du RSSI :

- Reconnaître et soutenir le RSSI : intervenir pour légitimer le rôle du RSSI vis-à-vis de la direction ou du service ;
- Sensibiliser les agents publics pour l'application du référentiel de sécurité (PSSI, procédure, charte, etc.) ;
- Adopter un comportement ayant valeur d'exemple en respectant les mesures de sécurité de la PSSI ;
- Exercer une surveillance permanente et informe le RSSI de toute situation anormale ou présomption d'incident ou de comportement à risque ;
- Participer aux arbitrages réalisés par le RSSI en cas de contrainte organisationnelle ou technique au sein d'une équipe.

Les directeurs sont également responsables des risques au niveau de leur périmètre. Ils valident le niveau de risques SI acceptable de chaque activité dont ils ont la charge, valident la mise en œuvre et font appliquer les mesures de sécurité des SI

adéquates, en allouant les ressources en cohérence avec les objectifs et la PSSI.

Pour cela, les directeurs s'appuient sur les travaux réalisés par le RSSI et le Délégué à la protection des données (DPO) pour obtenir les informations nécessaires afin de décider du caractère acceptable ou non des risques.

4.1.5. Utilisateurs internes

Chaque utilisateur interne du système (collaborateurs, chercheurs, enseignants, étudiants, stagiaires, prestataires, vacataires, etc…) respecte les règles de sécurité édictées par la PSSI et par la charte informatique, respecte les dispositifs et les mesures de sécurité, informe le RSSI de tout incident ou anomalie constatée.

4.1.6. Direction du Numérique (DN)

Les équipes de la DN assurent le développement et le fonctionnement des ressources informatiques et de télécommunication. Ils mettent en œuvre les services de sécurité des SI et de contrôle, en conformité avec la PSSI et pour répondre aux exigences formulées par les directions et les départements métiers.

Ils définissent et mettent en application les plans d'action techniques pour :

- L'intégration des règles et mesures de sécurité des SI dans leurs activités ;
- L'intégration des mesures de sécurité en phase de conception de chaque projet (Security By Design) ;
- La détection et la réaction en cas d'incident informatique.

Les équipes de la DN respectent les procédures internes, communes à toute la DN, afin de garantir :

- Une cohérence des activités au sein de la DN ;
- Un niveau de sécurité homogène entre les différents composants du SI, quel que soit l'équipe en charge de la mise en place et de l'exploitation en sein de la DN ;
- Le respect des mesures de sécurité de la PSSI.

Par défaut, la DN est le garant de l'application des mesures de sécurité pour tous les composants du système d'information de l'URCA inscrit dans son périmètre de contrôle. Lorsqu'un périmètre est géré par une autre direction pour des raisons organisationnelles ou techniques, un correspondant sécurité est nommé formellement pour appliquer les mesures de sécurité. Ce transfert se fait sous forme d'une attestation signée par les acteurs concernés.

Cette attestation précise :

- Le périmètre concerné : Description détaillée des composants du système concerné ;
- Les raisons justifiant le transfert de responsabilité ;
- Le responsable qui sera en charge du respect des règles de la PSSI : Le correspondant sécurité ;
- Les modalités de contrôle par le RSSI ;
- Les signatures et leurs rôles/responsabilités : au minimum, le RSSI/DN, le responsable de la direction concernée, et le correspondant sécurité désigné.

4.1.7. Correspondant sécurité des SI de recherche

Pour les besoins de la recherche, les équipes de l'URCA sont souvent amenées à déployer des systèmes dédiés à la recherche et qui ne sont pas contrôlés par les processus et procédures internes de la DN.

Pour assurer la sécurité des SI de recherche, conformément aux objectifs stratégiques de l'URCA, les composants du système d'information dédié à la recherche, qui ne sont pas dans le périmètre de la DN, sont mis sous la responsabilité d'un correspondant sécurité nommé pour chaque périmètre.

Au moment de la mise en place d'un système dédié à la recherche, une décision est prise par le RSSI, pour nommer un correspondant sécurité du système créé. Cette décision est prise conjointement avec :

- Le responsable du département concerné ;
- L'équipe de recherche concernée et son représentant ;
- L'équipe DN concernée.

Chaque composant non pris en charge par la DN dispose ainsi d'un correspondant sécurité qui prend en charge la responsabilité de sécuriser le composant conformément aux objectifs stratégiques de l'URCA. Cette information est documentée par le RSSI et maintenue à jour.

Les responsabilités du correspondant sécurité sont les suivantes :

- Décliner les règles de la politique de sécurité de l'URCA au niveau du composant recherche en prenant en compte les spécificités des procédés de recherches et les contraintes techniques et opérationnelles ;
- Coordonner le déploiement des mesures de sécurité au niveau du composant du SI de recherche ;

- Prendre en charge les mesures de sécurité opérationnelles (Durcissement, Mise à jour de sécurité, analyser des alertes, gérer les incidents, contrôler les droits d'accès, etc.)
- Assurer le relais avec la fonction centrale de cybersécurité portée par le RSSI (Reporting, capitaliser sur les solutions éprouvées, partager les retours d'expérience, etc.)

4.2. Le pilotage de la sécurité

4.2.1. Comité stratégique de la sécurité des SI

Un comité stratégique de la sécurité des systèmes d'information se réunit une fois annuellement. Ce comité réunit le RSSI et le Directeur Général ou tout autre membre du comité de direction. Il permet d'assurer :

- Le suivi et l'amélioration continue de la sécurité au niveau de l'URCA ;
- Le suivi des règles de la politique de sécurité ;
- Le suivi des travaux de mise en conformité réglementaire et contractuelle ;
- De maintenir à jour la Direction Générale du niveau de risque cyber qui pèse sur l'URCA ;
- La mise à disposition les ressources nécessaires pour assurer la conformité aux règles de la Politique de Sécurité des Systèmes d'Information ;
- Le suivi et la revue des processus de sécurité (Gestion des risques, Gestion d'incident, Gestion de la continuité d'activité, etc.).

4.2.2. Comité de Pilotage de la sécurité des SI

Le comité de pilotage de la sécurité des systèmes d'information se réunit au minimum tous les deux mois. Ce comité réunit le RSSI, le DN et les éventuels acteurs de l'URCA concernés par les thématiques abordées. Les sessions de ce comité de pilotage sont l'occasion de :

- Suivre l'avancement et l'exécution des plans d'action de la sécurité des systèmes d'information ;
- Valider les mesures de sécurité proposées pour la gestion des risques ;
- Obtenir les arbitrages et orientations dans les choix concernant la sécurité des systèmes de l'URCA ;
- Assurer le suivi des indicateurs sécurité ;

- Discuter des contrôles et audits relatifs à la sécurité des systèmes d'information.

4.2.3. Tableaux de bord de suivi

Le pilotage de la sécurité implique la mise en place d'une structure de suivi et induit la mise en place de tableaux de bord. Ces tableaux de bord sont réalisés par le RSSI et sont présentés au comité stratégique et doivent intégrer des indicateurs relatifs :

- Aux risques de sécurité ;
- Au taux d'application de la politique de sécurité ;
- Aux nombres d'incidents de sécurité rencontrés.

4.3. Relations avec les autorités

Des relations appropriées avec les autorités compétentes sont entretenues par le RSSI et le DPO. La procédure de gestion d'incident définit :

- Quand et comment contacter les autorités compétentes
- Comment signaler dans les meilleurs délais les incidents liés à la sécurité de l'information (tels que par exemple une tentative d'intrusion ou une fuite des données à caractère personnel)

Les utilisateurs ne sont pas autorisés à contacter par eux-mêmes les autorités, sauf à y être autorisé du fait de leur fonction, à condition d'informer immédiatement leur responsable qui feront remonter l'information aux RSSI et DPO.

5. Principes & processus de sécurité

L'URCA appuie la sécurité de ses systèmes d'information sur des processus permettant leur amélioration continue et leur ajustement à l'évolution des missions, du cadre réglementaire et des menaces pesant sur ses environnements numériques. Les principaux processus sont décrits ci-dessous.

Les processus de la présente politique, fixant un cadre général, se valent indépendants des technologies et des mécanismes de sécurité. Elles sont donc complétées par des instructions et mesures de sécurité, sous forme de politiques opérationnelles, qui déclinent au niveau opérationnel les principes fondamentaux.

5.1. Gestion des risques et conformité

L'URCA prend en compte les risques pouvant affecter ses systèmes d'information à différents niveaux :

- **Risques stratégiques :** Une analyse des risques globale, qui couvre tous les périmètres de l'URCA, est élaborée et maintenue à jour. Elle propose une vision macro des risques qui pèsent sur les systèmes d'information et permet de formaliser les règles de la politique de sécurité de l'URCA. Elle sert à mettre à jour tous les 3 ans la PSSI opérationnelle ;
- **Risques propres à un système :** Si nécessaire, chaque sous-système d'information de l'URCA peut fait l'objet d'une analyse des risques spécifiques en prenant en compte le contexte et l'écosystème du périmètre étudié ;
- **Risques projets informations « Security By Design » :** Chaque projet doit faire l'objet d'une appréciation des risques SSI afin d'élaborer les objectifs sécurité du projet. Ces objectifs sont traduits en exigences sécurités, intégrées dans le cahier des charges et dont le bon respect est contrôlé par le RSSI.

L'URCA élabore et maintient à jour une étude de conformité avec les lois, réglementations et engagements contractuels. Les non-conformités sont identifiées, partagées avec la Direction Générale et associées à des plans d'action SSI.

Pour le cas particulier du Règlement Général sur la Protection des Données (**RGPD**), le RSSI maintient à jour l'étude de conformité conjointement avec la Déléguée à la Protection des Données (DPO) de l'URCA.

5.2. Sélection et application des mesures de sécurité

Les mécanismes de sécurité mis en place au sein de l'URCA sont issus :

- Du processus de gestion des risques ;
- Du processus de conformité avec les lois, réglementations et engagement contractuel ;
- Des politiques de sécurité internes.

Ils sont sélectionnés par le RSSI conformément aux objectifs de sécurité fixés, en prenant en compte le contexte de l'URCA.

Les mécanismes de sécurité retenus, qu'ils soient de nature technique ou organisationnelle, sont alors applicables par toutes les parties prenantes des systèmes d'information de l'URCA.

La mise en place des mesures de sécurité techniques et organisationnelles est suivie par le RSSI au moyen de plan d'action SSI, régulièrement présentées à la Direction Générale.

5.3. Gestion des incidents de sécurité

Les incidents de sécurité sont identifiés, détectés, traités, évalués et leurs causes recherchées. Cette gestion est indispensable à l'amélioration continue de la sécurité ; elle est assurée par le RSSI, avec le concours des acteurs de la DN et des parties prenantes des directions concernées.

5.4. Audit et amélioration continue

L'activité d'audit est primordiale pour vérifier la bonne mise en œuvre des démarches et mesures de sécurité décrites dans les différentes politiques de sécurité des systèmes d'information de l'URCA.

Des audits de sécurité sont réalisés annuellement, particulièrement sur les activités essentielles de l'URCA.

Les audits de sécurité sont préparés, pilotés et analysés par le RSSI, en concertation avec les acteurs du système d'information concerné par le périmètre de chaque audit.

Les plans d'action d'audit sont proposés par l'auditeur en concertation avec le RSSI et validés par la Direction Générale. Le RSSI assure le suivi de la mise en place des plans d'action issus de chaque audit.

5.5. Sensibilisation et formation

Dans la sécurité, les comportements et la vigilance des personnes sont toujours un facteur majeur du succès ou d'échec. C'est un élément majeur de prévention de la survenue d'incidents et de limitation de ses impacts en cas de survenance.

L'URCA mène donc des actions de sensibilisation et de formation sous l'égide du RSSI.

5.6. Accès par des tiers et sous-traitance

Tout accès, qu'il soit physique ou logique, local ou à distance, aux ressources et informations de l'URCA par des tiers est accordé dans un cadre strict en fonction des besoins de la mission.

Les accès sont formellement approuvés par le collaborateur de l'URCA auquel ils sont rattachés et le RSSI, et fait l'objet d'un encadrement contractuel via la signature du contrat, où doit être systématiquement annexé les clauses liées à la sécurité des systèmes d'informations.

Les intervenants externes travaillent sous la responsabilité d'un collaborateur de l'URCA.

Les tiers et sous-traitants doivent en conséquence respecter ces clauses sous peine d'une pénalité ou d'une rupture de prestation, selon les conditions énoncées par l'URCA dans le contrat en question.