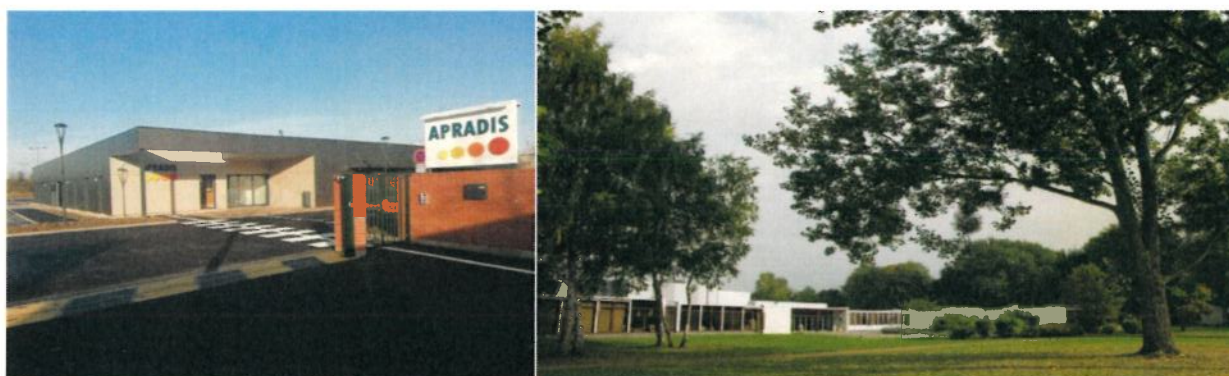


RÈGLEMENT INTÉRIEUR ETUDIANTS/ STAGIAIRES APRADIS



Association pour la **P**rofessionnalisation, la **R**echerche, l'**A**ccompagnement et le **D**éveloppement en Intervention **S**ociale
6-12 rue des Deux Ponts - 80000 AMIENS
Téléphone : 03 22 66 33 99 Fax : 03 22 52 61 99 - Site Internet : www.apradis.eu

Organisme de Formation enregistré sous le numéro d'activité **22 80 00052 80** auprès du préfet de région des Hauts-de-France



Préambule

Le présent règlement s'adresse à toutes les personnes, ci-après dénommées « étudiants/stagiaires, inscrites dans le cadre d'une formation au sein de l'APRADIS quel que soit leur statut (étudiant, en contrat d'apprentissage, en accompagnement VAE, ...) et ce, pour la durée de la formation suivie.

Conformément à la législation en vigueur, le présent règlement intérieur précise notamment le fonctionnement et les aspects réglementaires applicables à l'ensemble des étudiants/stagiaires accueillis au sein de l'APRADIS (ci-après dénommé « l'organisme de formation »), en vue de permettre le déroulement des actions de formation dans les meilleures conditions possibles et d'atteindre les objectifs formatifs, dans le respect de chacun et de l'environnement.

Le règlement intérieur repose notamment sur les valeurs et principes suivants :

- l'obligation pour chaque stagiaire de participer à toutes les activités correspondant à sa formation et d'accomplir les tâches qui en découlent,
- la prise en charge progressive par les étudiants/stagiaires eux-mêmes de la responsabilité de certaines de leurs activités, c'est-à-dire une implication individuelle alliée à une volonté collective d'investir réellement les obligations d'éducation et de formation proposées par l'organisme de formation dans l'application des articles du code du travail,
- le devoir de tolérance et de respect d'autrui dans sa personnalité et dans ses convictions,
- les garanties de protection contre toute agression physique ou morale et le devoir qui en découle pour chacun de n'user d'aucune violence.

Article 1

PARTICIPATION/ IMPLICATION

1.1 Assiduité

La présence à toutes les situations pédagogiques prévues dans le parcours de formation du stagiaire est strictement **OBLIGATOIRE**.

Les étudiants/stagiaires ne peuvent s'absenter, pendant les heures de stage ou de formation, qu'en cas de circonstances exceptionnelles, et avec un accord préalable écrit de la direction ou du responsable de la formation.

Au début de chaque séquence de formation, chaque stagiaire doit **obligatoirement** émarger sur une attestation de présence. Il est rappelé que le stagiaire ne peut signer que **pour lui-même**. (CF. note « fraude à la signature du 22 février 2016)

L'assiduité est systématiquement contrôlée. Une attestation de suivi de formation/ attestation de présence est délivrée en fin de cursus et elle est remise à l'autorité de certification.

Si le stagiaire est salarié, un courrier précisant ces modalités est envoyé à l'employeur et au centre de formation par l'apprentissage.



Il est précisé que l'organisme de formation se réserve le droit de présenter ou non le stagiaire aux épreuves de certification selon son parcours de formation (assiduité, non restitution des travaux, fraude, plagiat, ...), et ce, à tout moment de son parcours de formation.

1.2 Horaires

Les heures d'ouverture de l'APRADIS sont les suivants :

SITE AMIENS : 07h00 – 19h30

SITE LAON : 8h00-18h00

SITE BEAUVAIS : 8h00-18h00

Les étudiants/stagiaires doivent se conformer aux horaires de formation suivants sur l'ensemble des sites de formation de l'APRADIS : **9h00-12h30/ 13h30-17h00**

Une pause de 15 minutes est prévue chaque demi-journée.

Il est précisé que le non-respect de ces horaires peut entraîner des sanctions.

Sauf circonstances exceptionnelles justifiées, il est précisé que les étudiants/stagiaires ne peuvent s'absenter pendant les heures de formation et les heures de stage pratique.

Des horaires spécifiques pourront être appliqués. Dans ce cas, ils feront l'objet d'une information préalable.

1.3 Ponctualité- Absences

Chaque stagiaire veillera à être ponctuel pour garantir le bon déroulement de la formation.

Tout intervenant peut refuser une personne en retard pour la séquence de travail en cours. Dans cette situation, la personne devra rester au sein de l'organisme de formation et attendre la fin de la séquence.

Cette absence devra faire l'objet d'une compensation pédagogique.

En cas d'absence ou de retard, le stagiaire doit avertir, dans les plus brefs délais, l'intervenant ou le secrétariat administratif et pédagogique qui a en charge la formation.

Il est précisé que le justificatif, relatif aux absences, doit obligatoirement être fourni dans les 48 heures au plus tard. Il est à noter qu'une compensation pédagogique sera demandée (travail compensatoire).

Lorsque les étudiants/stagiaires sont des salariés en formation, l'APRADIS informe l'employeur de ces absences. Le stagiaire est également tenu d'informer son employeur. Toute absence ou retard, non justifiés par des circonstances particulières et/ou exceptionnelles, peut constituer une faute passible de sanctions disciplinaires.

En outre, pour les étudiants/stagiaires demandeurs d'emploi rémunérés par l'Etat ou une Région, ou pour les personnes en formation par la voie de l'apprentissage, les absences non justifiées entraîneront, en application de l'article R.6341-45 du Code du Travail, une retenue de rémunération proportionnelle à la durée desdites absences.



1.4 Accident

Tout accident ou incident survenu à l'occasion, ou en cours de formation doit être immédiatement déclaré par le stagiaire accidenté ou les personnes témoins de l'accident, auprès du secrétariat administratif et pédagogique qui a en charge la gestion de la formation.

Conformément à l'article R.6342-3 du Code du Travail, l'accident survenu au stagiaire au sein de l'Organisme de formation ou pendant qu'il s'y rend ou en revient, fait l'objet d'une déclaration par le secrétariat administratif et pédagogique de l'organisme de formation auprès de sa Caisse Primaire d'Assurance Maladie.

Article 2

DROITS ET OBLIGATIONS DES ETUDIANTS/STAGIAIRES

2.1 Règles de fonctionnement général

Les droits reconnus aux étudiants/stagiaires sont notamment le droit de publication et d'affichage, le droit d'association, le droit d'expression, le droit de réunion et le droit à la représentation.

Ces droits s'exercent dans le respect du pluralisme, du principe de neutralité et du respect d'autrui, et ne doivent pas porter atteinte aux activités d'enseignement, au déroulement des programmes et à l'obligation d'assiduité.

2.2 Droit de publication et d'affichage

Des panneaux d'affichage sont mis à la libre disposition des étudiants/stagiaires au sein :

- du bâtiment A pour le site d'Amiens,
- Sur le site de Beauvais,
- Sur le site de Laon.

Il est interdit d'afficher tout document ou annonce en dehors des lieux prévus à cet effet.

Tout propos injurieux, diffamatoire, calomnieux, mensonger ou portant atteinte aux droits d'autrui ou à l'ordre public dans une publication est de nature à engager la responsabilité de son ou de ses auteurs. En pareil cas, la direction peut suspendre ou interdire la parution ou l'affichage de la publication.

La publicité commerciale, la propagande politique, syndicale ou religieuse, sont interdites dans l'enceinte de l'organisme de formation, sauf autorisation préalable et écrite de la direction.

2.3 Droit d'expression individuelle

L'organisme de formation est laïc. Cela implique :

- La neutralité vis à vis de toutes les idées politiques, syndicales, religieuses ou philosophiques,
- L'exclusion de toute propagande et de tout prosélytisme,
- La tolérance et le respect d'autrui, dans sa personnalité, sa dignité et ses convictions.



Toutes les libertés individuelles sont respectées au sein de l'organisme de formation, notamment les libertés d'opinion et d'expression, dans le respect de la législation et de la réglementation en vigueur.

Chaque stagiaire a la possibilité de prendre contact avec la direction de l'association pour étudier les moyens de concilier au mieux ses convictions personnelles avec les nécessités de fonctionnement de l'organisme de formation.

Il est cependant rappelé que l'exercice des libertés individuelles ne peut conduire les étudiants/stagiaires à ne pas respecter leurs obligations (assiduité, restitution de travaux, respect des horaires, etc...).

Le prosélytisme est strictement interdit. Il est également interdit aux étudiants/stagiaires de tenir des propos injurieux ou excessifs à l'égard de l'un de leur collègue ou d'un tiers en raison de sa religion et, plus généralement de ses convictions personnelles.

2.4 Droit de réunion

Le droit de réunion est reconnu :

- ✓ aux associations agréées par le Conseil de perfectionnement (direction apprentissage),
- ✓ aux groupes de étudiants/stagiaires pour des réunions qui contribuent à l'information des autres étudiants/stagiaires.

Le droit de réunion s'exerce dans les conditions suivantes :

- ✓ chaque réunion doit être autorisée préalablement par le directeur de l'organisme de formation à qui l'ordre du jour doit être communiqué en même temps que la demande des organisateurs. L'autorisation peut être assortie de conditions à respecter,
- ✓ La réunion ne peut se tenir qu'en dehors des heures de formation des participants et aux heures d'ouverture du site,
- ✓ La participation de personnes extérieures à l'organisme de formation n'est pas admise,
- ✓ La réunion ne peut avoir un objet publicitaire, commercial, religieux ou politique.

Sur demande faite auprès du directeur de l'organisme de formation, une salle peut être attribuée en vue de la tenue d'une réunion.

2.5 Droit à l'image

Le droit à l'image est acquis par toute personne sur sa propre image. Ce droit permet avant tout à celui ou celle dont l'image est utilisée de refuser ou autoriser sa diffusion.

Dans le cadre des activités organisées par l'organisme de formation, des photographies et/ou vidéos pourront être prises.

En conséquence, est annexée au présent règlement intérieur une autorisation de diffusion de photographie et de vidéo (annexe 2), que le stagiaire signera et retournera auprès des secrétaires administratives et pédagogiques en charge de sa formation.



2.6 Participation des étudiants/stagiaires à la promotion de leur formation

Tout stagiaire suivant une formation dans l'organisme de formation peut être appelé à faire la promotion de sa formation et rendre compte de son expérience dans le cadre des actions de promotion et de développement mises en œuvre par l'organisme de formation ou à la demande de ses partenaires (Conseil Régional, organisme paritaire, ..).

2.7 Tenue

Une tenue vestimentaire décente et une hygiène correcte est exigée de la part des étudiants/stagiaires, comparable à la tenue exigée en structure d'accueil.

2.8 Obligation de règlement des frais pédagogiques et obligations diverses

Le stagiaire s'engage à remettre à l'organisme de formation les documents demandés et ce, dans les plus brefs délais.

Article 3

RESPONSABILITE COLLECTIVE ET INDIVIDUELLE

3.1 Accès aux locaux

Les étudiants/stagiaires doivent respecter les lieux d'entrée et de sortie des locaux, ainsi que les flux de circulation tels qu'ils leur seront précisés lors de leur accueil. Ils n'ont accès aux locaux qu'aux fins de formation aux horaires prescrits, sauf dérogation prévue par le présent règlement intérieur ou autorisation écrite et préalable de la direction.

L'accès aux salles de cours se fait uniquement en présence de l'intervenant ou sous la responsabilité du responsable de formation et pendant les horaires de formation.

L'accès à l'organisme de formation est interdit à toute personne extérieure aux actions de formation ainsi qu'aux animaux, sauf avec l'autorisation écrite et préalable de la direction. Il est également interdit de procéder à la vente de biens ou de services dans les locaux.

3.2 Circulation et stationnement

Les circulations et stationnements au sein du domaine de l'APRADIS sont réglementés. Sur le parking, les étudiants/stagiaires roulent lentement, manœuvrant avec prudence et stationnant aux endroits prévus, dans le respect des dispositions du code de la route.

Des emplacements de stationnements sont prévus pour les étudiants/stagiaires.



Des emplacements nominatifs sont strictement réservés au stationnement des véhicules du personnel et d'autres aux personnes en situation de handicap. Ces emplacements se doivent d'être respectés par tous.

Il est également précisé que les étudiants/stagiaires ne peuvent, ni réserver, ni utiliser les véhicules de service de l'association.

3.3 Distributeurs de boissons

Des distributeurs de boissons sont à la disposition des étudiants/stagiaires. Leur utilisation ne doit pas provoquer de perturbations ni nuire à la propreté de l'établissement. Les gobelets utilisés devront être déposés dans les poubelles prévues à cet effet.

3.4 Propreté

Chaque groupe est responsable de la propreté de la salle qu'il occupe : celle-ci devra donc être rangée et propre à la fin de chaque cours. Les étudiants/stagiaires ne sont pas autorisés à séjourner, durant les pauses, dans les salles de cours/ateliers ou à y consommer nourriture ou boissons sauf en salle 75 du bâtiment A sur le site d'Amiens sous réserve du respect des locaux.

3.5 Responsabilité collective et développement durable

Il est demandé à chacun d'adopter un comportement responsable quant à la gestion et à la consommation de l'énergie (eau, électricité, chauffage), quant à l'utilisation des consommables (papier, gobelets, plastiques, ...).

Chacun est concerné par la propreté des locaux et se doit de respecter le travail des services d'entretien.

3.6 Perte ou vol

Il est rappelé que chacun est responsable de ses affaires personnelles. En conséquence, l'organisme de formation décline toute responsabilité en cas de perte, de vol ou de détérioration d'objets personnels de toute nature déposés ou utilisés par les étudiants/stagiaires dans son enceinte (salle de cours, locaux administratifs, parcs de stationnement...).

Cependant, toute disparition doit être immédiatement signalée auprès du responsable de la formation.

Il est expressément recommandé de n'apporter aucun objet de valeur ni somme d'argent importante et de ne rien laisser sans surveillance dans les salles de cours.

3.7 Téléphone

L'utilisation d'un téléphone mobile pendant les séances de formation est **strictement INTERDITE**.

Les téléphones mobiles doivent être éteints et rangés pendant les séances de formation sous peine de sanction disciplinaire.

3.8 Duplication

L'intervenant fournit à chaque stagiaire les documents nécessaires à l'atteinte des objectifs pédagogiques.

3.9 Fraude et plagiat

Toute fraude (tricherie, plagiat, substitution de personnes, ...) commise durant le parcours de formation, dans le cadre de jurys internes ou de certification entraîne une sanction disciplinaire pouvant aller jusqu'à l'exclusion de l'Organisme de formation.

Concernant le plagiat, les règles communément admises sont :

- la citation de ses sources et de manière précise ; lorsque l'on cite un auteur (reproduction littérale d'un texte) la citation doit être repérée (italique et/ou mise entre guillemets) et référencée avec soin en note de bas de page ou dans le corps du texte ; toute citation sans guillemets et sans appel de note est un plagiat,
- La reprise d'une idée originale développée par autrui doit être signalée de manière à permettre au lecteur d'identifier l'auteur et de retrouver les documents où il l'a développée ;
- Il est obligatoire de référencer les sites internet qui ont été consultés et de repérer les passages reproduits de manière littérale.

Le plagiat est considéré comme une fraude. Il peut donc faire l'objet d'une sanction disciplinaire.

4 Consignes de sécurité et d'hygiène

4.1 Consignes générales

Outre le respect des règles de fonctionnement général, l'attention de chacun est appelée sur le respect des normes d'hygiène et de sécurité.

Elles concernent notamment :

- le signalement immédiat des accidents corporels ou matériels,
- l'observation des consignes d'évacuation données en cas d'alerte telles qu'elles sont affichées,
- le respect de tout protocole mis en place par l'Organisme de Formation.

Conformément à l'article R.6352-1 du Code du travail, lorsque la formation se déroule dans une entreprise ou un établissement déjà doté d'un règlement intérieur, les mesures de santé et de sécurité applicables aux étudiants/stagiaires sont celles de ce dernier règlement.

A ce titre, il est précisé que ces informations sont consultables :

- au sein de chaque bâtiment du site d'Amiens,
- au sein du site de Beauvais,
- au sein du site de Laon.

4.2 Interdiction de fumer

Conformément au décret n° 2006-1386 du 15 novembre 2006, paru au journal officiel le 16 novembre 2006, **il est strictement interdit de fumer dans les locaux de l'APRADIS.**

Il faut entendre par locaux, les lieux affectés à un usage collectif, accueillant du public ou qui constituent des lieux de travail (dont les bureaux).

Il est précisé :

- que la loi prévoit des sanctions consistant en une amende d'un montant forfaitaire de 68€ pour le contrevenant,
- que des sanctions disciplinaires pourront être prononcées à l'encontre des personnes ne respectant pas l'interdiction.

Le décret vise à protéger les personnes victimes du tabagisme passif, et à ce titre, il appartient à chacune et à chacun de rappeler, si nécessaire, aux contrevenants éventuels les termes de l'interdiction visée ou de saisir le responsable de la formation pour faire part des difficultés rencontrées dans la mise en œuvre de ces mesures.

Par respect pour les non-fumeurs, l'APRADIS veillera, conformément aux dispositions légales, à ce que l'interdiction de fumer soit scrupuleusement respectée.

4.3 Interdiction de « vapoter »

Conformément à l'article L.3511-7-1 du code de la santé publique, les mêmes dispositions s'appliquent concernant le « vapotage ».

A ce titre, **il est strictement interdit de « vapoter » dans les locaux de l'APRADIS.**

Il faut entendre par locaux, les lieux affectés à un usage collectif, accueillant du public ou qui constituent des lieux de travail (dont les bureaux).

Dans ces deux cas, il est rappelé que les fumeurs ne peuvent s'absenter pour fumer ou vapoter que pendant leur pause.

Pour des raisons de santé, de sécurité et pour l'image de l'association, les étudiants/stagiaires sont tenus de fumer ou de vapoter **uniquement** dans les zones « fumeurs » indiquées par l'APRADIS et ils doivent veiller à la propreté des lieux (notamment l'utilisation des cendriers).

4.4 Boissons alcoolisées et drogues

L'introduction et la consommation de boissons alcoolisées au sein de l'organisme de formation sont interdites.

Il est également interdit de laisser des personnes entrer ou séjourner au sein de l'association en état d'ivresse (C. trav., art. R. 4228-21).



En cas de constatation d'un état d'ivresse, l'organisme de formation contactera les services de secours (le 15) afin de faire cesser le risque provoqué par cet état d'ébriété.

Les services de secours, en fonction de l'état de santé de la personne concernée, indiqueront à l'organisme de formation les modalités à suivre.

L'organisme de formation pourra mettre en œuvre les mesures nécessaires pour assurer le retour à domicile du stagiaire concerné, à ses frais.

La consommation, la distribution et l'introduction de produits stupéfiants, au sein de l'organisme de formation sont interdites.

L'arrivée et/ou le maintien au sein de l'organisme de formation en état d'imprégnation de produits stupéfiants est interdite.

En cas de constatation, l'organisme de formation appellera les services de secours (le 15) afin de faire cesser le risque provoqué par cet état d'imprégnation de produits stupéfiants.

L'organisme de formation pourra mettre en œuvre les mesures nécessaires pour assurer le retour à domicile du stagiaire concerné, à ses frais.

Tout constat d'usage de stupéfiants sera signalé, sans délai, à un officier de police judiciaire.

Tout manquement à ces obligations pourra entraîner la mise en œuvre d'une sanction disciplinaire.

4.5 Consignes d'incendie

Les consignes d'incendie, et notamment un plan de localisation des extincteurs et des issues de secours, sont affichées dans les locaux de formation de manière à être connus de tous les étudiants/stagiaires qui doivent obligatoirement en prendre connaissance.

Des démonstrations ou exercices sont prévus pour vérifier le fonctionnement du matériel de lutte contre l'incendie ainsi que les consignes de prévention d'évacuation.

Tout matériel de secours ou d'extinction doit être rendu libre d'accès. Aucun matériel de secours ne peut être manipulé hors incendie.

4.6 Matériels

Tout stagiaire est tenu de conserver en bon état l'ensemble du matériel qui lui est confié en vue de l'exécution de sa formation. Il ne doit pas utiliser ce matériel à des fins autres que pédagogiques.

Les outils et les machines ne doivent être utilisés qu'en présence d'un intervenant et/ou avec accord d'un membre du personnel habilité.

Toute anomalie dans le fonctionnement des machines et du matériel ou tout incident doit être immédiatement signalée auprès de l'intervenant ou du responsable de la formation.



La remise en ordre des objets et matériels utilisés pour les activités de formation incombe aux étudiants/stagiaires.

Il est interdit d'emporter des objets/ matériels appartenant à l'organisme de formation sans autorisation préalable et écrite, sous peine d'exclusion.

Des outils informatiques, exclusivement destinés aux activités de formation, sont mis à disposition de chacun afin de faciliter la préparation et la réalisation des travaux, tant individuels que collectifs. Tout stagiaire peut accéder à ces outils dans le respect des conditions définies par leurs règles d'utilisation (notamment la Charte d'utilisation d'internet affichée dans les salles informatiques).

Chaque étudiant/stagiaire s'engage à respecter également l'ensemble des dispositions de la charte informatique jointe en annexe 2 du présent règlement intérieur et qui a pour objet de fixer les règles d'utilisation des moyens et des ressources informatiques mises à leur disposition.

Il est formellement interdit aux étudiants/stagiaires de manipuler les alimentations électriques présentes dans les salles informatiques ou autres. En cas de problème, les étudiants/stagiaires devront immédiatement alerter la personne chargée de la sécurité dans l'établissement et dont l'identité est indiquée par voie d'affichage dans la salle informatique.

Le stagiaire a également accès au centre de documentation de l'organisme de formation. Il s'engage à respecter le règlement de fonctionnement qui lui est remis en début de formation.

Article 5

REPRESENTATION DES étudiants/stagiaires

5.1 Dispositions générales

Conformément à l'article L.6352-4 du Code du Travail, pour chaque formation d'une durée supérieure ou égale à 500 heures, il est procédé simultanément à l'élection d'un délégué titulaire et d'un délégué suppléant.

Pour les formations d'une durée inférieure à 500 heures, l'organisation d'élection de délégués est laissée à la libre appréciation du directeur adjoint concerné.

Les délégués sont élus pour la durée de la formation. Leur fonction prend fin lorsqu'ils cessent de participer à la formation, pour quelque cause que ce soit.

Si l'un des délégués (titulaire ou suppléant) cesse son mandat avant la fin de la formation, il est procédé à une nouvelle élection.



5.2 Election

L'élection des délégués est organisée, au plus tôt vingt heures et au plus tard quarante heures, après le début de la formation.

Le directeur de l'organisme de formation, ou son représentant, assure l'organisation du scrutin et veille à son bon déroulement. Le scrutin a lieu pendant les heures de formation et se déroule à bulletin secret au scrutin uninominal à deux tours.

Tous les étudiants/stagiaires sont électeurs et éligibles. Aucune condition d'âge ou de nationalité n'est exigée.

Les candidatures sont individuelles. Les candidats peuvent se déclarer le jour même de l'élection, aucune déclaration préalable n'est nécessaire.

Chaque électeur vote pour un titulaire et un suppléant. Si un candidat obtient la majorité absolue des suffrages au 1^{er} tour, il est déclaré élu et devient délégué.

Au second tour, le candidat qui obtient le plus de voix est déclaré élu comme second délégué.

Si aucun des candidats n'obtient la majorité absolue au 1^{er} tour, on procède à un second tour où la majorité relative suffit. Les deux candidats qui obtiennent le plus de voix sont déclarés élus.

En cas d'égalité du nombre de voix, le plus âgé des candidats est déclaré élu.

Le directeur de l'organisme de formation, ou son représentant, adresse un procès-verbal de carence, transmis au Préfet de région territorialement compétent, lorsque la représentation des étudiants/stagiaires ne peut être assurée.

5.3 Rôle des délégués

Les délégués font toute suggestion pour améliorer le déroulement de la formation et les conditions de vie des étudiants/stagiaires dans l'Organisme de formation.

Ils présentent toutes demandes, observations individuelles ou collectives relatives au déroulement de la formation, aux conditions de vie des étudiants/stagiaires, aux conditions de santé et de sécurité et à l'application du présent règlement intérieur.

Ils sont acteurs de la communication interne et contribuent au respect du présent règlement intérieur.

Outre le conseil de discipline évoqué dans l'article 6 de ce présent règlement, et conformément aux textes réglementant les différentes formations, il est institué :

- Un conseil technique et pédagogique pour les formations diplômantes,
- Un comité de liaison pour les UFA ES et ME.



Selon les règles spécifiques à chacune de ces instances, une représentation des délégués y siège et a qualité pour faire connaître les questions et observations des étudiants/stagiaires relevant de ces instances.

5.4 Assemblée générale des délégués

En plus de leur rôle de représentants des étudiants/stagiaires, les délégués les représentent lors de l'assemblée générale des délégués de promotion.

Cette assemblée est une instance consultative qui regroupe tous les délégués de l'Organisme de formation.

L'assemblée générale se réunit, sous la présidence du directeur de l'Organisme de formation ou de son représentant au moins deux fois par an, dont 1 fois avant le 31 décembre de chaque année.

Au cours de la 1ère réunion, les membres élisent leurs représentants au conseil d'administration, au conseil technique et pédagogique ainsi qu'au comité de liaison.

Article 6

SANCTIONS DISCIPLINAIRES

Tout manquement du stagiaire aux obligations du présent règlement intérieur pourra entraîner des sanctions disciplinaires.

Constitue une sanction disciplinaire, au sens de l'article R.6352-3 du Code du Travail, « toute mesure, autre que les observations verbales, prises par le directeur de l'organisme de formation ou par son représentant, à la suite d'un agissement du stagiaire considéré comme fautif, que cette mesure soit de nature à affecter immédiatement ou non la présence de l'intéressé dans le stage ou à mettre en cause la continuité de la formation qu'il reçoit ».

Les sanctions ont, autant que possible, un caractère de réparation et doivent tendre à empêcher que les mêmes fautes ne se reproduisent.

L'échelle des sanctions applicables aux étudiants/stagiaires ayant à répondre, selon la gravité des faits, d'une faute est la suivante:

1. **Un blâme,**
2. **Un avertissement écrit**
3. **Une exclusion temporaire** d'un à trente jours,
4. **Une exclusion définitive.**

Dans tous les cas, lorsque le manquement constaté revêt un caractère de gravité important, le directeur de l'Organisme de formation ou son représentant pourra décider d'une mise à pied conservatoire, dans l'attente de l'issue de la procédure disciplinaire conformément à l'article R.6352-7 du Code du travail.

Ces sanctions ne préjugent pas d'éventuelles poursuites judiciaires notamment en cas de dégradation ou plus généralement de délit caractérisé.



Le directeur de l'Organisme de formation, ou son représentant, peut prononcer seul un blâme ou un avertissement écrit à l'encontre d'un stagiaire.

Conformément à l'article R.6352-5 du Code du travail, le stagiaire, à l'encontre duquel le directeur de l'Organisme de formation, ou son représentant, envisage de prendre une sanction, en dehors des observations verbales, sera convoqué à un entretien par lettre recommandée avec accusé de réception ou remise en mains propres contre décharge lui indiquant la date, l'heure et le lieu de l'entretien ainsi que l'objet de la convocation.

Au cours de l'entretien, le stagiaire peut se faire assister par la personne de son choix, notamment le délégué de promotion. La convocation susmentionnée fait état de cette faculté.

Le directeur de l'Organisme de formation, ou son représentant, indique le motif de la sanction envisagée et recueille les explications du stagiaire.

Dans le cas où la sanction relative à une exclusion temporaire ou définitive est envisagée, le stagiaire est convoqué en conseil de discipline.

Celui-ci est composé :

- du directeur de l'Organisme de formation ou son représentant : celui-ci préside le conseil,
- d'un cadre pédagogique désigné par les représentants des cadres pédagogiques siégeant au Conseil technique et pédagogique,
- d'un représentant des étudiants/stagiaires siégeant au Conseil technique et pédagogique.

Le conseil de discipline est saisi par le directeur de l'organisme de formation, ou son représentant, après l'entretien susvisé.

Il se réunit au plus tard 8 jours après sa saisine et formule un avis sur la mesure d'exclusion envisagée.

Le stagiaire est avisé de cette saisine. Il pourra être entendu, à sa demande ou à la demande du conseil, par le conseil de discipline. Il peut, dans ce cas, être assisté par une personne de son choix, stagiaire ou salarié de l'organisme.

Sur décision de son président, le conseil de discipline peut entendre le responsable de la formation, le formateur référent du suivi de parcours de formation et/ou toute personne susceptible d'éclairer la situation soumise au Conseil. Il est précisé que ces personnes n'ont pas de voix délibératives.

Après avoir entendu les parties intéressées, le conseil de discipline adopte un avis à l'intention de la direction de l'Organisme de formation à qui appartient la décision de sanctionner. Cet avis doit être transmis dans le délai d'un jour franc après sa réunion.

Dans tous les cas, la sanction ne peut intervenir moins d'un jour franc ni plus de quinze jours après l'entretien.

Toute sanction fait l'objet d'une **décision écrite et motivée, notifiée au stagiaire** sous la forme d'une lettre recommandée avec accusé de réception ou remise en mains propres contre décharge.



Lorsqu'un agissement fautif a rendu indispensable une mesure conservatoire d'exclusion temporaire à effet immédiat, les dispositions de l'article R.6352-7 du Code du travail et, le cas échéant, du présent règlement intérieur devront être respectées.

La finalité de cette procédure est d'amener les étudiants/stagiaires concernés à s'interroger sur le sens de leur conduite, de leur faire prendre conscience des conséquences de leurs actes pour eux-mêmes et autrui et de leur donner les moyens de mieux appréhender le sens des règles qui régissent le fonctionnement de l'organisme de formation.

Le directeur de l'organisme de formation, ou son représentant, doit informer de la sanction prise :

- L'employeur, lorsque le stagiaire est un salarié bénéficiant d'une action de formation dans le cadre du plan de formation d'une entreprise,
- L'employeur et l'organisme paritaire agréé qui a pris en charge les dépenses de formation, lorsque le stagiaire est un salarié bénéficiant d'un congé individuel de formation,
- L'organisme collecteur paritaire agréé qui a assuré le financement de l'action de formation dont a bénéficié le stagiaire.

Article 7

DISPOSITIONS FINALES

Application

Le présent règlement intérieur est remis à chaque stagiaire avant son inscription définitive et tout règlement de frais.

Un exemplaire est également affiché dans chaque site et disponible au niveau de chaque secrétariat.

Tout le personnel de l'organisme de formation est chargé de veiller à son application.

Fait à Amiens, le **02/10/2024**





ANNEXE 1

BULLETIN DE SOUSCRIPTION OBLIGATOIRE
A RETOURNER COMPLETEE AUPRES DU SECRETARIAT ADMINISTRATIF ET PEDAGOGIQUE

Je soussigné (e) :

Demeurant à :

.....
.....
.....
.....

Formation suivie :

Certifie avoir pris connaissance du règlement intérieur pour les étudiants/stagiaires de l'APRADIS et m'engage à en respecter les termes.

Signature

(Précédée de la mention manuscrite « Lu et approuvé – Bon pour accord »)

A....., le.....



ANNEXE 2

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATIONS DE L'APRADIS (PSSI)

Sommaire

1. Préambule.....	18
1.1. Définitions.....	18
2. Portée et opposabilité	20
3. Champ d'application.....	20
3.1 Personnes concernées.....	20
3.2 Usages concernés.....	20
4. Conditions d'utilisation générales.....	21
4.1 Usage professionnel.....	21
4.2 Usage non professionnel.....	22
4.3 Conditions d'accès et d'identification.....	24
4.4 Gestion des absences et des départs.....	25
5. Conditions d'utilisation spécifique.....	26
5.1 Mobilité et accès distant.....	26
5.2 Télétravail.....	26
5.3 Gestion des connaissances et de l'espace collaboratif.....	26
5.4 Médias sociaux.....	26
6. Protection de la propriété intellectuelle, des informations et des données.....	27
6.1 Propriété intellectuelle et droit à l'image.....	27
6.2 Préservation du secret et de la confidentialité.....	28
6.3 Protection des données à caractère personnel.....	29
7. Sécurité et vigilance.....	31
7.1 Sécurité.....	31
7.2 Traçabilité.....	32
7.3 Filtrage.....	32



<u>7.4 Scan informatique</u>	32
<u>7.5 Mesures d'urgence et plan de reprise d'activité</u>	33
<u>8. Contrôle, maintenance et gestion des ressources</u>	33
<u>8.1 Contrôle et audit</u>	33
<u>8.2 Maintenance</u>	34
<u>8.3 Consommations</u>	34
<u>9. Responsabilité et sanctions</u>	35
<u>10. Information et entrée en vigueur</u>	36

1. Préambule

La présente charte a pour objet de fixer les règles d'utilisation des moyens et des ressources informatiques mises à la disposition des utilisateurs, ci-après définis à l'article 4.1, dans le cadre de leur activité professionnelle. Elle a pour vocation d'être diffusée à l'ensemble des personnels ainsi qu'aux utilisateurs occasionnels du système d'information de l'APRADIS.

Les règles ainsi définies sont destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance d'usage des systèmes d'information et de communication, en conformité avec les dispositions légales et réglementaires applicables ainsi que la jurisprudence des tribunaux.

Elle tient compte des obligations du Règlement général sur la protection des données (RGPD), des recommandations de la Commission nationale de l'informatique et des libertés (CNIL) et de celles de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La charte est rédigée dans le souci de concilier les intérêts de chaque utilisateur et ceux de l'APRADIS. Elle manifeste ainsi la volonté de l'APRADIS d'assurer un usage loyal, respectueux et responsable de ses systèmes d'information et de communication, ainsi que de protéger son patrimoine et son image de marque.

La charte est annexée au règlement intérieur (membre du personnel et étudiants/stagiaires). Elle pourra évoluer en fonction du contexte légal et de la politique de sécurité notamment applicable au sein de l'APRADIS. Elle est partie intégrante de la politique de sécurité des systèmes d'information (PSSI) de l'APRADIS dont elle constitue un premier élément. En tant que de besoin, des fiches techniques annexées à la PSSI ou à la présente charte viendront en préciser certains points.

1.1. Définitions

Au sens de la charte, les termes ci-dessous ont la signification suivante :

- « actif » : ordinateurs, photocopieurs, supports mobiles de conservation des données, serveurs, infrastructure réseau, système et logiciels d'application, données et autres sous-systèmes et composants.



Les « actifs informationnels » sont définis comme les systèmes d'information, les équipements informatiques, les téléphones mobiles, les supports de stockage de données, etc. Les documents papier font aussi partie des actifs informationnels ; les règles qui leur sont appliquées font l'objet d'un autre document : *Guide de bonnes pratiques pour la gestion des documents papier et du bureau vide*.

- « application » : logiciel de traitement automatisé de données numériques, accessible à partir du réseau interne de l'APRADIS ou par internet ;
- « backup » : solution de secours informatique pouvant être hébergée par l'APRADIS ou par un site extérieur ;
- « charte » : le présent document et ses annexes constituant la charte des systèmes d'information et de communication de l'APRADIS ;
- « code malveillant » : logiciel développé dans le but de nuire à un système informatique ou d'exfiltrer des données des utilisateurs (virus, vers, chevaux de Troie, keyloggers, etc.) ;
- « consommable » : produit ou constituant qui disparaît par l'usage des systèmes d'information et de communication (consommables d'impression, d'encre, fournitures de bureau diverses, etc...);
- « donnée à caractère personnel » : toute information relative à une personne physique identifiée ou identifiable (personne concernée), directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ;
- « filtrage » : ensemble d'outils informatiques visant à limiter l'accès à certains sites Internet en raison de leurs contenus (contrôle des contenus, des URL, protocolaire, etc.) ;
- « matériel nomade » : moyens informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux de l'APRADIS ;
- « moyen d'authentification » : moyen permettant l'accès aux systèmes d'information et de communication et pouvant prendre diverses formes : login/mot de passe, biométrie, signature électronique, cartes avec ou sans contact, etc. ;
- « scan » : contrôle à travers des outils informatiques de la présence de mots clés dans des contenus (dossiers, documents, courriers électroniques, pièces-jointes, fichiers, etc.) ;
- « service en ligne » : service de communication par voie électronique de mise à disposition du public ou de catégories de public, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondance privée ;
- « signe distinctif » : signe permettant l'identification d'une entreprise, d'un produit ou d'un service : marques, dessins et modèles, enseignes, nom commercial, dénomination sociale, nom de domaine, et faisant généralement l'objet d'une protection par le droit de la propriété intellectuelle ;
- « systèmes d'information et de communication » : ressources et moyens informatiques et moyen de communication électronique, recouvrant tout matériel informatique, câblage, périphériques (tels que imprimantes simples ou multifonctions, webcam, etc...), disque dur externe ou interne, carte mémoire, CD-Rom, clé USB, ordinateur, tablette, PDA, photocopieurs, scanner, etc... et toute ressource informatique de toute nature (logiciels, applications, bases de données, etc...), et ce, qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau, ainsi que les moyens de communication électronique recouvrant internet et les télécommunications (tels que téléphone, équipement sans fil, carte de communication sans fil, terminaux portables, le matériel nomade, messagerie, forum, sites web, etc...) ;

Association pour la **P**rofessionnalisation, la **R**echerche, l'**A**ccompagnement et le **D**éveloppement en **I**ntervention **S**ociale
6-12 rue des Deux Ponts - 80000 AMIENS

Téléphone : 03 22 66 33 99 Fax : 03 22 52 61 99 - Site Internet : www.apradis.eu



- « trace informatique » : donnée informatique témoignant de l'existence d'une opération au sein d'une application ou du système d'information ;
- « webmail » : service de messagerie accessible par l'intermédiaire d'un navigateur internet, qui permet donc l'émission, la consultation et la manipulation de courriers électroniques ;

2. Portée et opposabilité

La charte étant annexée aux différents règlements intérieurs, elle est applicable de fait et produit, à ce titre, les mêmes effets.

3. Champ d'application

3.1 Personnes concernées

La charte est applicable, et donc opposable aux collaborateurs de l'APRADIS, salariés permanents ou intervenants occasionnels, aux étudiants/stagiaires quel que soit leur statut, ainsi qu'aux bénévoles de l'association, aux prestataires et sous-traitants, au personnel mis à disposition d'en prendre connaissance afin d'en respecter les principes et obligations. Les sanctions prévues pour les mésusages sont décrites dans cette charte.

Sont visés par la charte :

- l'ensemble des systèmes d'information et de communication qui sont la propriété de l'APRADIS ou qui sont mis à la disposition des utilisateurs à des fins professionnelles ou tout autre nouveau système qui serait mis en place ;
- l'ensemble des systèmes d'information et de communication qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu auprès d'une personne habilitée (directeur ou responsable) une autorisation d'utilisation dans le cadre de son activité professionnelle.
- Chaque utilisateur est propriétaire des actifs qui lui sont confiés. En ce sens, il est responsable de la confidentialité, de l'intégrité et de la disponibilité de l'information incluse dans ses actifs.

3.2 Usages concernés

La charte s'applique à tous les types d'usage de moyens et de ressources informatiques et numériques, quelle que soit leur fréquence ou leur périodicité, et qu'ils aient lieu :

- dans les locaux de l'APRADIS, quelle que soit leur localisation ;
- dans le cadre d'un usage dit « nomade », quel qu'en soit le lieu ;
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès (domicile, etc.)

4. Conditions d'utilisation générales

Les actifs informationnels sont mis à la disposition des utilisateurs par le service Informatique et systèmes d'informations, sous la responsabilité du responsable de ce service. Seul le personnel de ce service est habilité à gérer les actifs informationnels et à intervenir en mode administrateur sur les appareils. Il est le seul habilité à installer des logiciels et applications sur le matériel, ou à les supprimer. Il est le seul à pouvoir mettre en service les actifs et à en assurer la maintenance.

Les mises à jour des logiciels et systèmes d'exploitation sont automatiques via les éditeurs de logiciels (Suite Office, Suite Adobe, Panda, Microsoft) ou sont réalisées manuellement à chaque demande faite par l'éditeur (Cegid, Ypareo). Une veille sur l'obsolescence des systèmes d'exploitation et des logiciels est en outre réalisée par le service informatique et système d'informations.

Un numéro unique d'identification est apposé sur chaque actif informationnel par le service Informatique et systèmes d'informations. Ce dernier détient la liste de tous les actifs, incluant leur dénomination, leur numéro unique d'identification, leur durée d'utilisation et la date probable de leur remplacement.

Chaque utilisateur est propriétaire des actifs qui lui ont été remis. Il doit en ce sens en assurer la sécurité, tant pour les actifs de bureau que pour les actifs nomades et supports d'information. Chaque fois que la responsabilité de la perte ou de la détérioration d'un actif et des informations qu'il contient est imputable à l'utilisateur, celui-ci encourt les sanctions prévues ci-après.

4.1 Usage professionnel

4.1.1 Systèmes d'information et de communication de l'APRADIS

Les systèmes d'information et de communication quelle que soit leur nature, sont réservés à un usage professionnel et sont donc présumés avoir un caractère professionnel, quelles que soient les conditions effectives d'utilisation.

Selon la jurisprudence, sont présumés avoir un caractère professionnel, notamment :

- les fichiers créés par un utilisateur grâce aux systèmes d'information et de communication de l'établissement, sauf lorsque celui-ci les identifie comme étant « personnel » ;
- les connexions établies par un utilisateur sur des sites internet pendant son temps de travail grâce aux systèmes d'information et de communication de l'établissement ;
- les clés USB dès lors qu'elles sont connectées à un outil informatique mis à la disposition de l'utilisateur par l'APRADIS.

Il en résulte que :

- l'APRADIS peut y accéder hors de la présence de l'utilisateur, pour des raisons de continuité d'activité ou par mesure de sécurité ;
- aucune information à caractère professionnel ne peut être ni stockée dans un répertoire informatique utilisé à des fins non professionnelles, ni émise ou reçue *via* le courrier électronique non professionnel.



Messagerie électronique. En particulier, l'adresse électronique, composée de « prénom.nom@apradis.eu », est professionnelle. Elle ne doit donc pas être utilisée dans un autre contexte, et être notamment diffusée sur des services en ligne, sans rapport avec l'activité professionnelle.

Services en ligne et applications. L'accès à des services en ligne et applications est également réservé à un usage professionnel.

4.1.2 Moyens personnels de l'utilisateur

L'utilisateur ne peut utiliser à des fins professionnelles des systèmes d'information et de communication qui sont sa propriété personnelle ou qu'il détient à titre personnel, sans obtenir une autorisation préalable auprès du responsable du service informatique et systèmes d'information, pour toute connexion aux réseaux de l'APRADIS.

4.2 Usage non professionnel

Bien que les systèmes d'information et de communication de l'APRADIS soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles est tolérée.

Cette tolérance pourra être suspendue ou limitée en cas d'abus.

Un tel usage non professionnel ne doit pas :

- perturber le bon fonctionnement des systèmes d'information et de communication de l'APRADIS ;
- compromettre ses activités et particulièrement ses missions d'intérêt général et la continuité de l'activité ;
- porter atteinte aux obligations qui incombent aux utilisateurs compte tenu de leur statut et notamment, les obligations de dignité, de loyauté, de discrétion, de neutralité ou de réserve ;
- porter atteinte ou être susceptible d'engager la responsabilité de l'APRADIS ;
- poursuivre un but lucratif ;
- porter atteinte à l'image de marque ou à la réputation de l'APRADIS.

L'usage non professionnel des systèmes d'information et de communication se traduit dans les faits par :

- la possibilité de créer un répertoire informatique non professionnel ;
- la possibilité d'utiliser à des fins non professionnelles la messagerie électronique professionnelle (pour rappel « prénom.nom@apradis.eu »).

Afin de garantir la confidentialité des répertoires et messages électroniques non professionnels, il est impératif que l'utilisateur utilise le terme « PERSONNEL » :

- sur le répertoire informatique ;
- dans la zone objet du message électronique ;
- si le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée, sms...), le message à caractère non professionnel doit débuter par le terme « PERSONNEL ».



A défaut d'utiliser le terme « PERSONNEL », tous les répertoires informatiques et tous les messages informatiques sont considérés comme professionnels.

L'utilisateur est entièrement responsable de l'usage des systèmes d'information et de communication de l'APRADIS à des fins privées et dégage en conséquence l'APRADIS de toute responsabilité.

Le caractère non professionnel de l'usage des systèmes d'information et de communication interdit, par principe, à l'APRADIS, d'accéder aux contenus ou données émis, reçus ou échangés dans ce cadre.

Le caractère non professionnel du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce que :

- l'APRADIS puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour l'établissement de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;
- ces éléments fassent l'objet de conservation technique dans le cadre de la mise en œuvre des sauvegardes planifiées par le service informatique et systèmes d'information.

En cas de détection ou de suspicion de la présence d'un code malveillant, il soit procédé :

- à la mise en quarantaine ou le cas échéant, à la suppression de l'élément quelconque qui comporterait un code malveillant ;
- à ce qu'une personne du service informatique et systèmes d'information accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des systèmes d'information et de communication, notamment dans le cadre d'opérations de maintenance ;
- à ce que l'APRADIS puisse, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'il y est autorisé par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.)

L'utilisation du système d'information et de communication à titre non professionnel doit être non lucrative et raisonnable quant à sa fréquence, sa durée et dans la mobilisation des ressources matérielles mises à disposition des utilisateurs.

Cette utilisation ne doit pas nuire à la qualité du travail ni au temps qui y est consacré. Elle doit respecter la réglementation en vigueur.

Il est ainsi rappelé, que ce soit à titre professionnel ou non professionnel, qu'il est interdit de se connecter sur des sites à caractère pornographique, pédopornographique, zoophile, injurieux, violent, raciste, antisémite ou nazi, d'incitation à la haine ou à la violence ou à la commission d'acte illicite, discriminatoire, diffamatoire, faisant l'apologie du terrorisme, ou manifestement contraire à l'ordre public ou de télécharger ou visionner ou stocker ou transmettre, etc. des contenus de telle nature. L'utilisateur dont ces faits seraient avérés s'expose à des sanctions disciplinaires voire judiciaires, reprises ci-après.



Chaque utilisateur est doté d'un ou de plusieurs moyens d'authentification permettant l'accès aux moyens et ressources informatiques et numériques.

Les moyens d'authentification sont confidentiels. En aucun cas, ces informations doivent être disponibles et visibles à proximité du matériel. Les moyens d'authentification ne peuvent donc être :

- écrits et collés sur le matériel ;
- rangés dans un tiroir de bureau, une armoire ;
- inscrits dans un document quelconque y compris sur une feuille volante.

Il est, dès lors, interdit à l'utilisateur :

- de procéder à la moindre divulgation à un tiers ou à un autre utilisateur, même intra-service, de son ou de ses moyens d'authentification ;
- d'utiliser un moyen d'authentification autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;
- de supprimer, masquer ou modifier son identité ou son identifiant ;
- d'user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès ;
- lorsqu'un accès distant lui est accordé, d'utiliser d'autres moyens d'authentification que ceux qui lui sont remis à cet effet.

Les mots de passe doivent être robustes et modifiés régulièrement. Ils doivent se conformer à la politique de mot de passe édictée conformément aux prescriptions du RGPD transcrites par la CNIL relativement à la protection des données personnelles et notamment :

- être composé d'au moins 8 caractères ;
- ces caractères doivent être une combinaison de caractères d'au moins 3 des 4 types suivants : majuscules, minuscules, chiffres, caractères spéciaux ;

L'utilisateur doit impérativement modifier son mot de passe tous les trois mois (90 jours). Un message automatique apparaîtra en temps voulu sur l'écran de l'ordinateur de l'utilisateur afin de modifier le mot de passe.

Lorsqu'un matériel est inactif depuis 2 minutes, celui-ci se verrouillera automatiquement, nécessitant la saisie du moyen d'authentification pour le déverrouiller. D'une manière générale, l'utilisateur veillera à verrouiller le matériel (ordinateur, photocopieur, etc.) dès lors qu'il s'absente.

En ce qui concerne la sécurité et la confidentialité, l'utilisateur devra suivre toutes les prescriptions complémentaires qui lui seront signifiées par le service informatique et systèmes d'information.

4.3.1 Incident, perte, vol ou compromission

Dès lors qu'un utilisateur constate un incident lié à l'utilisation d'un actif placé sous sa responsabilité, ou si ses moyens d'authentification ont fait l'objet d'une communication ou qu'il existe un risque qu'ils aient été communiqués, ou en cas de vol, ou de suspicion de compromission de ses moyens d'authentification,

Association pour la Professionnalisation, la Recherche, l'Accompagnement et le Développement en Intervention Sociale
6-12 rue des Deux Ponts - 80000 AMIENS

Téléphone : 03 22 66 33 99 Fax : 03 22 52 61 99 - Site Internet : www.apradis.eu



L'utilisateur doit contacter immédiatement le service informatique et systèmes d'information de l'APRADIS et avertir son responsable hiérarchique avec copie à la Direction générale adjointe, de la perte ou du vol d'un équipement informatique dont il a l'usage, afin qu'une étude d'impacts soit menée. Il devra également, selon les cas, soit assister l'APRADIS, soit procéder lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit. Cet incident doit aussi être inscrit par l'utilisateur concerné, ou le cas échéant par son supérieur hiérarchique, dans le tableau créé dans le cadre de la démarche qualité afin que soit assuré le suivi de l'action corrective.

Selon la réglementation en vigueur issue du RGPD, tout incident touchant à l'intégrité des données, à leur disponibilité ou à leur confidentialité, notification devra être faite à la CNIL dans les 72 heures et, selon les conventions ou accords signés, avec les financeurs et pouvoirs adjudicateurs dans les délais qui seraient les leurs. Dans ce cas précis, une information sera faite aux collaborateurs ayant à traiter ces données particulières.

Cet acte d'information est de nature à dégager la responsabilité de l'utilisateur pour les agissements qui auraient lieu post-déclaration.

En cas d'incident, l'APRADIS se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer le droit d'accès de toute personne aux systèmes d'information et de communication. Elle s'efforcera, autant que faire se peut, de prévenir l'utilisateur concerné dans des délais raisonnables, notamment en cas de maintenance.

4.4 Gestion des absences et des départs

En cas d'absence ou de départ de l'utilisateur, l'APRADIS se réserve le droit de mettre en place une solution de re-routage des messages électroniques ou toute autre solution technologique permettant d'assurer la continuité de l'activité du service.

En cas d'absence de l'utilisateur, pour quelque raison et durée que ce soit, l'APRADIS se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement tout document à caractère professionnel de l'utilisateur.

Lors de son départ, l'utilisateur doit :

- supprimer, au plus tard, la veille de son départ les répertoires et les messages électroniques nommés « PERSONNEL », ainsi que tous les documents de même nature. A défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments sont automatiquement supprimés sans être consultés et sans qu'aucune copie ne soit réalisée.

Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder trois (3) mois, le compte messagerie de l'utilisateur, ainsi que ses moyens d'authentification, sont désactivés au plus tôt.



5. Conditions d'utilisation spécifique

5.1 Mobilité et accès distant

Dans le cadre de ses déplacements professionnels, quelle que soit leur durée ou leur fréquence, l'utilisateur assure la garde et la responsabilité des actifs informationnels dont il a la propriété.

Ainsi, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations, données et ressources du système d'information de l'APRADIS qu'il pourrait être amené à manipuler ou à échanger. En cas d'incident avéré ou de doute, l'utilisateur doit immédiatement en aviser le service informatique et systèmes d'information.

5.2 Télétravail

L'utilisation autorisée au télétravail devra suivre les dispositions de la charte ainsi que l'ensemble des procédures et instructions données par l'APRADIS pour l'utilisation des systèmes d'information et de communication. La connexion aux systèmes d'information de l'APRADIS se fera via le VPN (réseau virtuel privé).

5.3 Gestion des connaissances et de l'espace collaboratif

Chaque utilisateur s'engage à être attentif à la pertinence des informations diffusées au sein des espaces collaboratifs. Il veille, notamment, à s'informer des règles de diffusion d'un document, notamment lorsqu'il s'agit d'informations nominatives ou à caractère personnel.

Par souci de qualité, de responsabilité et de protection du patrimoine informationnel de l'APRADIS, l'utilisation de ces mêmes espaces et outils peut faire objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

5.4 Médias sociaux

Les réseaux sociaux permettent aux utilisateurs de créer de nouvelles relations professionnelles et d'optimiser les échanges professionnels autour de leurs projets. Cependant, leur utilisation peut être source de risques et de responsabilité notamment en termes d'image, ou de fraude. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

5.4.1 Usage professionnel

Dans le cadre de la sphère professionnelle, l'utilisateur doit obtenir au préalable l'autorisation de son supérieur hiérarchique pour pouvoir participer à un réseau social, ou créer un espace sur un réseau social au nom de l'APRADIS.



Si l'autorisation a été donnée, l'utilisateur doit se conformer aux règles et instructions édictées par son supérieur hiérarchique, ce dernier étant seul compétent pour déterminer les conditions d'utilisation du réseau social.

De plus, lorsqu'un réseau social est utilisé, l'utilisateur devra :

- s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de l'APRADIS ;
- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image de l'APRADIS ;
- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables (notamment en matière de concurrence, de consommation et de propriété intellectuelle, de droit de la presse, de propos illicites) ;
- utiliser uniquement les outils de communication de l'APRADIS, selon les instructions qui lui ont été données;
- s'abstenir de diffuser toute information confidentielle ou toute information commerciale sensible relative à l'APRADIS ou à ses partenaires ;
- prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour les systèmes d'information et de communication de l'APRADIS.

En cas de doute sur l'utilisation d'un réseau social, l'utilisateur devra immédiatement consulter son supérieur hiérarchique.

L'autorisation donnée pourra être retirée, modifiée ou suspendue par le supérieur hiérarchique dès lors que l'intérêt de l'APRADIS le justifie.

5.4.2 Usage non professionnel

Dans le cadre de la sphère non professionnelle et hors les murs de l'établissement, l'utilisateur est bien évidemment libre d'utiliser les réseaux sociaux. Cependant, il s'interdit de communiquer la moindre information sur son activité professionnelle, en particulier des informations confidentielles et des informations sensibles relatives à l'APRADIS ou à ses partenaires.

6. Protection de la propriété intellectuelle, des informations et des données

6.1 Propriété intellectuelle et droit à l'image

L'utilisation des systèmes d'information et de communication de l'APRADIS implique le respect des droits de propriété intellectuelle et du droit à l'image.

Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- utiliser les logiciels et applications, dans les conditions de la licence souscrite par l'APRADIS ;
- ne pas effectuer de copie illicite de logiciel ou d'applications et, a fortiori, de tenter d'installer des logiciels ou applications pour lesquels l'APRADIS ne posséderait pas un droit d'usage ;



- ne pas reproduire, copier, utiliser remettre à des tiers ou diffuser, les bases de données, pages web, dessins, modèles, logos ou autres créations de l'APRADIS ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles, sans autorisation ou licence ;
- ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des utilisateurs ou de tiers à l'APRADIS.

6.2 Préservation du secret et de la confidentialité

6.2.1 Règles générales

La sauvegarde des intérêts de l'APRADIS nécessite le respect par l'utilisateur d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et des données dont il a connaissance dans le cadre de l'exercice de son activité professionnelle.

Le respect de cette obligation implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations et données ;
- n'accéder qu'aux informations et données en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres utilisateurs ;
- ne pas extraire ces informations et données confidentielles et ne pas les reproduire ou les détourner de leur utilisation normale à des fins non professionnelles ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein de l'APRADIS.

La diffusion de toute information ou donnée confidentielle ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect d'une procédure sécurisée.

6.2.2 Chiffrement

Il est interdit aux utilisateurs de chiffrer les répertoires, dossiers ou boîtes ou libellés à caractère privé ou non professionnel.

6.3 Protection des données à caractère personnel

6.3.1 Devoirs des utilisateurs

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » en vigueur et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018, dit Règlement général sur la protection des données.

Dans ce cadre, les utilisateurs devront informer le délégué à la protection des données (DPD), fonction assurée par la société DataVigiProtection et se conformer à la procédure en vigueur pour la mise en œuvre d'un traitement de données à caractère personnel.

Conformément à la législation applicable à la protection des données personnelles, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un traitement de données personnelles sont les suivants :

- le respect des finalités initiales du traitement ;
- la pertinence, la complétude et l'exactitude des données au regard des finalités poursuivies ;
- l'information des personnes à la collecte des données et la conservation du recueil de leur consentement en cas de signature électronique ou manuscrite;
- le droit d'accès, de rectification ;
- le droit d'opposition ;
- la mise en œuvre de mesures de sécurité adaptée à la sensibilité des données traitées, résultant d'une étude d'impact pour les personnes privées en cas de divulgation, altération ou destruction des données les concernant.
- le contrôle rigoureux de la diffusion de données à caractère personnel à l'attention de tiers extérieurs, en incluant notamment les clauses adaptées dans les contrats avec les sous-traitants.
- la destruction des données dès la fin de la période de conservation prévue.

L'Apradis s'est doté d'un logiciel modulaire de gestion des étudiants/stagiaires (Ypareo) qui respecte les standards du RGPD. L'accès à Ypareo se fait par login et mot de passe, différents de ceux de la session d'ouverture du PC.

6.3.2 Droits des utilisateurs

L'APRADIS met en œuvre des traitements de données à caractère personnel en relation avec l'usage et la sécurité des systèmes d'information et de communication couverts par la présente charte. L'APRADIS s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.



L'APRADIS a désigné un délégué à la protection des données externalisé : DataVigiProtection.

Les catégories suivantes de données sont traitées :

- informations professionnelles ;
- informations relatives à l'identité ;
- coordonnées professionnelles ;
- logs de connexion et autre trace informatique ;
- informations sur l'utilisation des systèmes d'information et de communication.

Ces catégories de données proviennent essentiellement des systèmes d'information et de communication ainsi que des annuaires informatiques et de la direction des ressources humaines.

Ces données sont conservées selon les durées légales.

Ces données sont destinées à l'APRADIS ainsi qu'aux personnes habilitées au sein de l'établissement et aux autorités habilitées.

Les traitements opérés dans le cadre de la charte ont pour finalité :

- le suivi et la maintenance des systèmes d'information et de communication, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
- la gestion des annuaires et référentiels permettant de définir les autorisations d'accès aux applications et réseaux ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des systèmes d'information et de communication, notamment la conservation des logs de connexion, des traces informatiques et des données de toute nature, analyser automatiquement, notamment à des fins d'historisation et de preuve de l'utilisation des systèmes d'information et de communication ;
- la gestion de la messagerie électronique ;
- le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation, de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;
- le contrôle du respect de la charte et les audits de sécurité ;
- les statistiques, investigations et enquêtes.

Ces finalités permettent à l'APRADIS de répondre à la sauvegarde de ses intérêts vitaux, à ses obligations légales ou contractuelles, à la poursuite de missions d'intérêt public ou à ses intérêts légitimes liés à la bonne utilisation et à la sécurité de ses systèmes d'information et de communication dans le respect des droits des utilisateurs.

A toutes fins utiles, il est rappelé que les données collectées auprès des utilisateurs sont obligatoires aux fins de bonne gestion, d'organisation et de sécurité des systèmes d'information et de communication.



Conformément à la loi « Informatique et libertés » modifiée transcrivant le RGPD, les utilisateurs sont informés, en particulier, qu'ils disposent d'un droit d'interrogation, d'accès, de limitation, d'effacement, de rectification et d'opposition au traitement des données les concernant et qui s'exerce auprès du délégué à la protection des données (DataVigiProtection). Par ailleurs, les utilisateurs disposent d'un droit de réclamation auprès de la Cnil.

7. Sécurité et vigilance

7.1 Sécurité

A des fins de précaution, certaines configurations peuvent être verrouillées par l'APRADIS (poste de travail, accès internet, etc.)

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des systèmes d'information et de communication mis à sa disposition, principalement en évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information de l'APRADIS.

L'utilisateur doit se conformer aux règles de conduite suivantes :

- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou douteux ;
- ne pas modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit ;
- ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes d'information et de communication ou aux réseaux à travers les matériels dont il a usage ;
- ne pas utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;
- ne pas effectuer des opérations pouvant nuire aux relations internes ou externes de l'APRADIS.

En cas de réception de messages non sollicités (spams), et notamment en cas de tentative de phishing visant à obtenir ses identifiants, l'utilisateur veille à :

- ne pas l'ouvrir sans s'être assuré préalablement de son innocuité ;
- ne pas y répondre ;
- ne pas le transférer ;
- informer le service informatique et systèmes d'information;
- agir sur instruction du service informatique et systèmes d'information.

L'utilisateur s'efforcera de signaler, sans délai, tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les systèmes d'information et de communication.

Un antivirus (Panda) est mis en œuvre sur l'ensemble des PC avec une mise à jour automatique. Les serveurs sont protégés en tête de connexion sur les 3 sites par un pare-feu (PFSENSE).

7.2 Traçabilité

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à apporter la preuve, le cas échéant, du bon usage des systèmes d'information et de communication mis à la disposition des utilisateurs, l'APRADIS met en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des systèmes d'information et de communication.

Les traces informatiques sont conservées pour une durée limitée d'un an.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

7.3 Filtrage

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de ses systèmes d'information et de communication, l'APRADIS se réserve le droit de mettre en place des outils de filtrage permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre certaines catégories de sites internet ou d'applications.

Ces outils, en ce qu'ils portent entre autres sur l'accès à internet, permettent un contrôle des connexions des utilisateurs.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

7.4 Scan informatique

L'APRADIS se réserve le droit de mettre en œuvre des opérations de scan des systèmes d'information et de communication tels que le scan des éléments professionnels de l'utilisateur, et notamment des documents, des dossiers, des courriers électroniques, pièces jointes, fichiers.

Les outils de scan informatique n'ont pas pour objet l'ouverture des éléments identifiés. Ils permettent à l'APRADIS de disposer d'un dispositif d'alerte prudentiel et rapide de ses systèmes d'information et de communication.

Les documents, dossiers, courriers électroniques, pièces jointes, etc. identifiés comme « PERSONNEL » ne seront pas consultés par l'APRADIS, sauf dans le cadre des dispositions légales particulières de la jurisprudence en la matière et de la charte.

Dans la mesure où le déploiement d'Ypareo est en cours à la date de mise en œuvre de la Charte informatique, la saisie des informations à caractères personnels se fait par transcription du papier. Un échantillonnage des saisies est réalisé pour s'assurer de la validation des données saisies. Cette opération sera inutile par la saisie des informations directement par les étudiants/stagiaires sous Ypareo.

7.5 Mesures d'urgence et plan de reprise d'activité

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, l'APRADIS peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la ou de la reprise de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené, à la demande de l'APRADIS, à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, télétravail, déplacement sur des sites de secours tiers, etc.).

8. Contrôle, maintenance et gestion des ressources

8.1 Contrôle et audit

Les opérations de contrôle et d'audit portent sur la régularité de l'utilisation des systèmes d'information et de communication. Elles se justifient par les obligations incombant à l'APRADIS.

En effet, de par son activité, l'APRADIS est soumise à une obligation générale de sécurité, en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, et de la loi dite « Informatique et Libertés » modifiée.

L'APRADIS, en tant qu'employeur, dispose également d'un pouvoir de contrôler l'activité des utilisateurs et en particulier, le respect par eux de la charte.

L'utilisation des moyens et ressources informatiques et numériques pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

L'APRADIS se réserve ainsi le droit, notamment :

- de vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;
- de contrôler l'origine licite des logiciels installés ;
- de conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.



En outre, en cas d'incident, l'APRADIS se réserve le droit de :

- surveiller le contenu des informations qui transitent sur son système d'information ;
- vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisateurs ;
- procéder à toutes copies utiles pour faire valoir ses droits.

Tout intervenant en charge de contrôles ou d'audit doit impérativement respecter la confidentialité des échanges électroniques et des fichiers des utilisateurs. Quand il s'agit d'un prestataire externe, la signature d'une clause de confidentialité est demandée.

Les utilisateurs sont toutefois informés que le service informatique et systèmes d'information est conduit, de par sa fonction et selon des procédures déterminées, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexions à internet, etc...), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail.

Néanmoins, le service informatique et systèmes d'information est tenu au secret professionnel et ne peut utiliser son droit d'administrateur qu'à des fins strictement professionnelles.

En cas de non-respect avéré de la charte par un utilisateur, et suivant la gravité des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus par l'APRADIS.

8.2 Maintenance

La mise à disposition de moyens et ressources informatiques et numériques implique nécessairement des opérations de maintenance technique (maintenance corrective, maintenance préventive ou évolutive), et ce, pour assurer le bon fonctionnement et la sécurité de ceux-ci.

Ces opérations prennent la forme d'une intervention d'une personne du service informatique et systèmes d'information, soit sur site, soit à distance, conduisant alors cette personne à effectuer une « prise en main à distance » selon un calendrier préétabli ou en cas d'incident.

En aucun cas, ces opérations, quel que soit leur mode opératoire, ne justifient le fait pour l'utilisateur de communiquer ses moyens d'authentification.

Dans ce cadre, la « personne habilitée » peut être amenée à prendre connaissance de l'ensemble des éléments présent sur le poste ou le matériel nomade de l'utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.

Si, à l'occasion d'opérations de maintenance, une utilisation anormale ou un contenu illicite ou préjudiciable sont identifiées, l'APRADIS en tirera toute conséquence.

8.3 Consommations

8.3.1 Règles de conservation, de sauvegarde et d'archivage électronique

Chaque utilisateur doit mettre en œuvre et organiser, selon les instructions de sa hiérarchie, les moyens nécessaires à la conservation des messages, des informations et des données de toute nature lorsque cela est nécessaire.



L'utilisateur est dans l'obligation de respecter les règles ou la politique de conservation et d'archivage de l'APRADIS.

Les traces détaillées d'activité sont conservées pendant les durées légales ou conventionnelles, à l'issue desquelles elles sont détruites.

Ces traces valent preuve de l'utilisation des systèmes d'information et de communication.

Ces traces peuvent faire l'objet d'un traitement statistique.

Ces traces peuvent être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

Les sauvegardes, backup et archivages électroniques concernant les éléments du répertoire et les messages nommés « PERSONNEL », sont conservés sous la seule et entière responsabilité de l'utilisateur.

9. Responsabilité et sanctions

L'utilisateur est responsable :

- dans le cadre de son activité professionnelle, de l'utilisation des moyens et ressources informatiques et numériques en conformité avec la présente charte ;
- dans la sphère de sa vie privée résiduelle, seul, à l'exclusion donc de toute responsabilité de l'APRADIS, de tout usage des moyens et ressources informatiques et numériques à caractère non professionnel.

Le non-respect des dispositions légales et réglementaires, ainsi que de la charte, expose l'utilisateur en cause à des sanctions disciplinaires, s'échelonnant du blâme au licenciement pour faute grave ou faute lourde avec perte du droit aux indemnités de préavis et de licenciement, ou à des poursuites judiciaires.

La rupture du principe de discrétion professionnelle ou la divulgation d'informations non anonymes sont passibles d'un an d'emprisonnement et 15 000 € d'amende (article 226.13 du code pénal). L'abus de confiance, caractérisant le détournement de données de collaborateurs, d'apprenants ou de bénévoles de l'APRADIS par un utilisateur est puni de trois ans d'emprisonnement et 375 000 € d'amende (art. 314-1 du code pénal).

Un utilisateur fournissant des informations à un tiers pour lui permettre de détourner les mesures de protection ou de sécurité pour se procurer les données ou un autre avantage au préjudice de l'APRADIS, se rend coupable d'escroquerie ou de complicité d'escroquerie et risque à ce titre cinq ans d'emprisonnement et 375 000 € d'amende (art. 313-1 du code pénal).

Un utilisateur ayant obtenu des données confidentielles ou à caractère personnel via le système d'information de l'APRADIS risque jusqu'à cinq ans d'emprisonnement et 75 000 € d'amende au titre de l'atteinte à un système de traitement automatisé de données (art. 323-1 et suivants du code pénal).

10. Information et entrée en vigueur

La présente charte, modifiant la version du 28 octobre 2022, a été adoptée par le bureau de l'Apradis (28 février 2023), le conseil d'administration de l'Apradis (21 mars 2023) et a été présentée pour information et consultation au CSE de l'Apradis (14 avril 2023).

Elle est ajoutée en annexe aux règlements intérieurs des membres du personnel, des étudiants/stagiaires et est envoyée aux partenaires et prestataires concernés.

Elle est applicable à compter du 1^{er} juin 2023.

Le propriétaire de ce document est Philippe Lorenzo, Directeur général, qui doit le vérifier et, le cas échéant, le mettre à jour.

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être pris en compte :

- nombre d'incidents liés au non-respect de la charte informatique ;
- nombre d'incidents liés à des oublis d'articles de la charte informatique.