

RÈGLEMENT INTÉRIEUR

EXTRAIT POUR ÉNAP ORGANISME DE FORMATION
ET DE DÉVELOPPEMENT DES COMPÉTENCES

Janvier 2025



SOMMAIRE

Préambule.....	2
TITRE 12 : Les formations organisées par l'Énap organisme de formation.....	3
Article 1 : Articles 76 à 77 du règlement intérieur de l'École équivalent au présent titre 12.....	3
Article 2 : Assiduité, ponctualité et absences (Extraits du TITRE 3 : La formation des élèves et stagiaires)	3
2.1 (Article 24 du RI Énap) : Assiduité et absences.....	3
Article 3 : Tenue et comportement (Extraits du TITRE 3 : La formation des élèves et stagiaires).....	3
3.1 (Article 26 du RI Énap) : Tenue des élèves, stagiaires et auditeurs.....	3
3.2 (Article 27 du RI Énap) : Comportement attendu.....	3
Article 4 : L'hébergement (Extraits du TITRE 4 : La vie sur le campus).....	3
4.1 (Article 39 du RI Énap) Affectation des chambres.....	3
4.2 (Article 40 du RI Énap) Hygiène et propreté	4
4.3 (Article 41 du RI Énap) Tranquillité et vie collective.....	4
Article 5 : La vie dans les lieux dédiés à la pédagogie (Extraits du TITRE 4 : La vie sur le campus).....	4
5.1 (Article 42 du RI Énap)	4
5.2 (Article 43 du RI Énap)	4
5.3 (Article 45 du RI Énap) : La médiathèque.....	4
Article 6 : Les autres structures (Extraits du TITRE 4 : La vie sur le campus).....	4
6.1 (Article 47 du RI Énap) Parkings et déplacements.....	4
6.2 (Article 48 du RI Énap) Structures dédiées à la culture, à la détente et aux loisirs.....	4
Article 7 : La sécurité du site (Extraits du TITRE 5 : La sécurité du site).....	5
7.1 (Article 50 du RI Énap) Accès au site de l'Énap.....	5
7.2. (Article 51 du RI Énap) Port du badge.....	5
Article 8 : Santé et sécurité (Extraits du TITRE 7 : La santé et la sécurité au travail).....	5
8.1 (Article 61 du RI Énap) Prévention d'accidents.....	5
8.2 (Article 64 du RI Énap) Prévention sanitaire.....	5
Article 9 : Représentation des stagiaires (selon les dispositions des articles R6352-9 à R6352-14 du code du travail).....	5
Article 10 : Discipline (Extraits du TITRE 6 – La discipline et selon les dispositions des articles R6352-3 à R6352-8 du code du Travail).....	5
10.1 (Article 57 du RI Énap) L'utilisation des moyens de communication et réseaux sociaux.....	5
10.2 (Article 58 du RI Énap) Procédure disciplinaire.....	6
10.3 (Article 60 du RI Énap) Responsabilités.....	6
Article 77 : Transmission du règlement.....	6
Article 78 : Application du règlement.....	6

Préambule

Conformément à l'article 8 du décret n° 2000-1328 du 26 décembre 2000 modifié relatif à l'école nationale d'administration pénitentiaire, le présent règlement intérieur fixe le cadre de vie à l'intérieur de l'établissement public à caractère administratif. Il s'applique à toutes les catégories de personnes accédant aux bâtiments publics situés sur le domaine de l'école nationale d'administration pénitentiaire (Énap) ou locaux loués pour des besoins pédagogiques.

Ce règlement intérieur précise les domaines de responsabilités des instances de direction (Conseil d'Administration, Conseil Pédagogique et Scientifique) et des instances de dialogue représentatives (Comité Technique, Comité d'Hygiène, de Sécurité et des Conditions de Travail). Il régit les relations entre les personnels et les administrateurs de cette école et constitue un instrument de régulation de ces relations dans un esprit de concertation.

Définitions des catégories de personnes accédant à l'Énap :

- > Les « élèves et stagiaires » sont en formation initiale ou continue.
- > Les « auditeurs » sont les personnes admises en Classe Préparatoire Intégrée.
- > Les « auditeurs étrangers » sont les personnes reçues dans le cadre des relations internationales de l'Énap.
- > Les « personnels de l'Énap » sont les fonctionnaires ou agents contractuels contribuant au fonctionnement de l'école.
- > Les « intervenants ou acteurs pédagogiques » sont les personnalités appartenant à l'administration pénitentiaire ou rattachées à d'autres organismes de formation, universités ou chercheurs indépendants ; ils sont sollicités pour délivrer des cours ou participer à des colloques.
- > Les « personnels des entreprises privées » assurent certaines fonctions comme la restauration, le nettoyage, la maintenance technique, l'entretien des parcs et jardins ou la sécurité.
- > Les « résidents » sont les élèves, stagiaires ou intervenants pédagogiques qui bénéficient d'un logement.
- > Les « passagers résidents » sont les fonctionnaires ou personnes extérieures au service public pénitentiaire qui par convention signée par la direction bénéficient d'un logement.
- > Les « passagers » sont les étudiants d'autres universités qui viennent se restaurer, ou bien les visiteurs ou invités à des cérémonies, actions sportives et socio-culturelles organisées par l'Énap ou encore des personnes qui accèdent par convention à certaines structures sportives ou dédiées à la pédagogie.
- > Les « personnes extérieures » sont toutes les personnes non précédemment définies qui pénètrent sur le site de l'École, quelle qu'en soit le motif et la durée.

Ce texte définit les droits et obligations de chacun en fonction des raisons de sa présence à l'école. Il est spécifié lorsque certains articles s'adressent plus particulièrement à l'une ou l'autre catégorie.

Ce règlement, porté à la connaissance de toutes les catégories de personnels au moment de leur arrivée, est mis en ligne sur les sites Internet et Intranet de l'école. Il

est opposable à tous. Il favorise l'instauration d'une vie commune fondée sur le respect mutuel, sur la devise de l'administration pénitentiaire « Honneur et Discipline » et sur l'application du code de déontologie pénitentiaire du 30 décembre 2010 modifié par le décret du 15 février 2016. Ce respect mutuel et la reconnaissance des valeurs républicaines sont consacrés par la déclaration du 10 octobre 2016, annexée au présent règlement, relative aux valeurs communes au Réseau des écoles du service (RESP) et aux valeurs spécifiques de l'Énap, en particulier l'exemplarité.

Le code de déontologie du service public pénitentiaire est affiché dans les locaux : il énonce les devoirs permettant à toutes les catégories de personnels d'argumenter une décision et d'adopter un comportement adapté suscitant la confiance de tous.

Les trois principes fondamentaux de fonctionnement at tendus sont la continuité du service public, le respect du principe de précaution et l'efficacité de l'action de service public.

La mise en pratique de ces principes et valeurs participe à la réalisation des objectifs assignés à l'école et à ceux assignés aux élèves, stagiaires et auditeurs, et contribue à l'instauration de relations non conflictuelles et courtoises.

Tout au long du texte l'utilisation du terme de « direction » fait référence au Directeur ou directrice de l'Énap.

TITRE 12 : Les formations organisées par l'Énap organisme de formation

Article 1 : Articles 76 et 77 du règlement intérieur de l'École équivalent au présent titre 12

Article 2 : Assiduité, ponctualité et absences (Extraits du TITRE 3 : La formation des élèves et stagiaires)

2.1 (Article 24 du RI Énap) : Assiduité et absences

2.1.1 (Article 24.1 du RI Énap)

Les élèves, stagiaires et auditeurs suivent avec assiduité et ponctualité l'ensemble des activités programmées dans leur emploi du temps.

Ils contrôlent régulièrement leur programme car il peut être modifié. Ils en sont informés sans délai et par tout moyen mis à leur disposition dès lors que le changement a lieu dans la semaine.

Les absences sont constatées par la direction de la formation. Les retards et absences sont pris en compte dans l'évaluation et une mention est portée dans le dossier administratif, pédagogique et le carnet de liaison.

2.1.2 (Article 24.2 du RI Énap)

Les absences admises sont celles des usagers qui en ont, à l'avance et sur justificatif — sauf urgence — obtenu l'autorisation de la direction en charge de la formation ou du responsable de leur unité de formation.

Dans l'impossibilité d'assister à une activité (urgence médicale ou sociale), l'usager informe, avant le début du cours et par tout moyen, l'unité de formation dont il dépend.

Article 3 : Tenue et comportement (Extraits du TITRE 3 : La formation des élèves et stagiaires)

3.1 (Article 26 du RI Énap) : Tenue des élèves, stagiaires et auditeurs

3.1.1 (Article 26.1 du RI Énap)

Une tenue correcte est exigée en permanence sur le site de l'école. L'aspect physique et vestimentaire soigné renvoie à l'image de dignité et d'autorité des fonctions déjà occupées ou assumées plus tard en fin de formation.

Tout insigne politique, philosophique ou religieux ne peut être ostensiblement arboré sur une tenue civile et est incompatible avec le port de l'uniforme. Les insignes réglementaires de l'administration pénitentiaire sont uniquement autorisés sur un uniforme.

Sauf autorisation spécifique de la direction de l'École, toute personne pénétrant sur le site de l'École doit veiller à la parfaite neutralité religieuse, philosophique ou politique des vêtements qu'elle porte. Le port de tout vêtement permettant l'expression publique de l'appartenance à une religion est strictement interdit

3.2 (Article 27 du RI Énap) : Comportement attendu

3.2.1 (Article 27.1 du RI Énap)

Le comportement des usagers et des personnels en raison de leur qualité de fonctionnaire de l'administration pénitentiaire est exemplaire en toutes circonstances à l'école ou hors de l'école. À l'Énap cela signifie que tous les personnels, élèves, stagiaires et auditeurs respectent les valeurs spécifiques de l'Énap figurant dans la déclaration du 10 octobre 2016 annexée au présent règlement :

> Tous les personnels, élèves, stagiaires et auditeurs de l'école se saluent sur le campus.

> Sont exclus tous propos injurieux, vulgaires, expressions discriminantes à connotations sexiste, raciste, homophobe ou concernant la situation de famille, l'apparence physique, le patronyme, l'état de santé, le handicap ou relevant des opinions politiques, philosophiques, religieuses ou syndicales.

> Il convient pour les personnels de l'école d'appliquer le devoir mutuel d'aide et assistance en s'interdisant tout jugement de valeur sur un collègue et en travaillant ensemble pour la réussite de tous, en respectant le travail de l'autre.

Sont strictement interdits les actes de prosélytisme, les manifestations de discrimination, les incitations à la haine et toute forme de pression physique et psychologique visant à

imposer un courant de pensée religieux, philosophique ou politique qui s'opposerait au principe de laïcité. Aucune raison d'ordre religieux, philosophique, politique ou en considération de sexe ne peut être invoquée pour refuser de participer à certains enseignements, empêcher d'étudier certains ouvrages ou auteurs, refuser de participer à certaines épreuves d'examen, contester les sujets, les choix pédagogiques ainsi que les formateurs.

3.2.2 (Article 27.2 du RI Énap)

Les usagers respectent le silence en salle de cours et en amphithéâtre.

3.2.3 (Article 27.3 du RI Énap)

Les résidents sont vigilants au repos des personnes dans les bâtiments dédiés à l'hébergement.

3.2.4 (Article 27.4 du RI Énap)

L'interdiction de consommer de l'alcool et tout produit illicite est absolue sur le campus sauf exception mentionnée à l'article 55.2.

Il est interdit de se trouver en état d'imprégnation alcoolique et/ou sous l'emprise de produits stupéfiants sur le campus de l'École, dès que l'on pénètre sur le site de l'École.

L'état d'imprégnation alcoolique peut être constaté :

> Par le personnel de l'Énap ayant reçu délégation, au moyen d'un éthylotest ou d'un éthylomètre, avec le consentement de l'agent, toutefois le refus de se soumettre à un tel contrôle emporte présomption d'état d'imprégnation alcoolique ;

> Par le personnel de l'Énap observant des signes d'ivresse manifeste comme l'incohérence des propos, des difficultés d'élocution ou de marche, une haleine alcoolisée.

La constatation de l'état d'imprégnation alcoolique peut entraîner :

> L'exclusion des activités,

> L'exclusion des hébergements,

> L'établissement d'une demande d'explication pouvant aboutir à des sanctions disciplinaires.

Une note de service précise les modalités d'exécution de ces constats.

3.2.5 (Article 27.5 du RI Énap)

Tous les déplacements des usagers se font dans le calme.

3.2.6 (Article 27.7 du RI Énap)

L'Énap attache une importance à la lutte contre toute forme de discrimination. La diffusion des valeurs républicaines grâce à la mobilisation des acteurs de la communauté pédagogique vise au renforcement du sentiment d'appartenance à la République et à l'institution pénitentiaire.

Article 4 : L'hébergement (Extraits du TITRE 4 : La vie sur le campus)

4.1 (Article 39 du RI Énap) Affectation des chambres

4.1.1 S'il a souhaité être hébergé à la signature de la convention de formation, une chambre individuelle, avec kit de toilette, est affectée au stagiaire moyennant paiement selon les conditions financières fixées par note de service.

Si des contingences structurelles ou ponctuelles, en raison de circonstances dues notamment à l'accueil de promotions conséquentes, empêchaient l'Énap d'assurer un hébergement individuel, la décision de ne pouvoir fournir un hébergement individuel devra être communiquée au stagiaire plus de deux semaines avant la date de la formation.

4.1.2 (Article 39.1 du RI Énap)

Les chambres sont affectées aux usagers ou passagers résidents nominativement et sous leur responsabilité. Il leur est interdit d'héberger une autre personne. L'École peut proposer des hébergements exclusivement réservés aux femmes ou aux hommes. Les modalités de cette mise en œuvre sont établies par note de service.

4.1.3 (Article 39.2 du RI Énap)

Un état des lieux, déclaratif est effectué par l'élève, stagiaire ou auditeur au moment de la prise de possession de la chambre et il est contradictoire en présence de personnes désignées par la direction au moment de sa restitution.

4.1.4 (Article 39.3 du RI Énap)

Toute demande de modification des conditions d'hébergement est écrite et fait l'objet d'une autorisation préalable par le chef d'unité accueil.

4.1.5 (Article 39.5 du RI Énap)

Les visites de chambres sont organisées par les personnes désignées par la direction. Elles sont réalisées en la présence du ou des occupants de la chambre. Elles permettent de s'assurer que les mesures du règlement intérieur sont respectées.

4.1.6 (Article 39.6 du RI Énap)

Un manquement grave aux règles de vie liées à l'hébergement peut donner lieu à la suppression de ce service par décision de la direction, ceci après avoir recueilli les observations de l'intéressé, sans préjuger des éventuelles suites disciplinaires. Dans ce cas, l'usager prend des dispositions pour se loger à ses frais.

4.2 (Article 40 du RI Énap) Hygiène et propreté**4.2.1 (Article 40.1 du RI Énap)**

Chaque usager ou passager résident observe les règles de propreté et d'hygiène indispensables à une vie en collectivité. Le nettoyage de la chambre incombe à l'occupant. Il est rappelé l'interdiction de fumer et/ou de vapoter dans tous les bâtiments y compris dans les chambres, ceci pour des raisons de sécurité incendie et pour permettre l'accueil de non-fumeur. Il est interdit d'utiliser des bougies, chauffages d'appoints ou tout autre objet dégageant de la chaleur ou utilisant un système de combustion. Le résident veille à la bonne aération de la chambre.

4.2.2 (Article 40.2 du RI Énap)

La confection de repas, l'utilisation de dispositifs permettant la cuisson, le réchauffage ou la conservation d'aliments sont interdits dans tous les locaux des bâtiments d'hébergement. Il est autorisé l'utilisation d'une bouilloire électrique. Toutefois, les résidents qui le souhaitent peuvent se rendre au local restauration aux horaires affichés afin de réchauffer un repas acheté. Dans ce local se trouve le mobilier répondant à ce besoin : chaises, tables, micro-ondes et réfrigérateurs.

4.2.3 (Article 40.3 du RI Énap)

Les animaux domestiques ne sont pas autorisés à l'intérieur des locaux de l'école, à l'exception des animaux ayant un rôle de guide ou de protection des personnes.

4.2.4 (Article 40.4 du RI Énap)

Le tri sélectif des déchets est obligatoire pour les usagers et passagers résidents. Les déchets sont jetés dans les conteneurs semi-enterrés situés sur les parkings à l'entrée de chaque village selon les préconisations fixées par les pictogrammes.

4.2.5 (Article 40.5 du RI Énap)

L'École s'inscrit dans la transition écologique et dans la réduction de son impact environnemental.

La réduction de la consommation des énergies et la diversification alimentaire sont, notamment, des thématiques inscrites dans sa politique de sobriété et de diminution de son empreinte écologique.

4.3 (Article 41 du RI Énap) Tranquillité et vie collective**4.3.1 (Article 41.1 du RI Énap)**

La vie collective en résidence.

Sauf autorisation exceptionnelle de la direction, toute activité collective est prohibée à compter de 22h30 dans les villages et leurs abords. Les comportements individuels générateurs de troubles à la tranquillité publique sont de même prohibés.

Toute personne hébergée sur le site veille au respect des locaux mis à sa disposition et des espaces verts. Les abords immédiats du bâtiment sont conservés dans un état de propreté entre chaque passage des sociétés de nettoyage des locaux et de jardinage.

Il est interdit de déplacer le mobilier (tables, chaises et fauteuils) des espaces communs et des chambres. L'espace citoyen qu'est notre école doit conduire chacun à adopter une attitude et un comportement responsables.

4.3.2 (Article 41.2 du RI Énap)

(L'intendant) Il fait respecter les prescriptions du règlement intérieur et, vis-à-vis de toutes les personnes présentes sur le campus, l'autorité que lui confère la direction pour dresser des observations ou prendre des mesures d'urgence. Il relate sans délai au cadre de permanence les circonstances de tout incident

grave, puis fait suivre un rapport écrit à la direction. L'intendant relève du service du Département Accueil Hébergement Pôle Sécurisation (DAHPS) et supervise la sécurisation du site.

Article 5 : La vie dans les lieux dédiés à la pédagogie (Extraits du TITRE 4 : La vie sur le campus)**5.1 (Article 42 du RI Énap)**

Chacun veille à la bonne conservation des locaux, du mobilier et du matériel mis à disposition et s'attache à respecter et à faire maintenir la propreté dans toutes les salles de cours, amphithéâtres, ainsi que dans les couloirs, escaliers et blocs sanitaires.

5.2 (Article 43 du RI Énap)

Formateurs et usagers respectent l'affectation des mobiliers se trouvant dans chaque salle de cours. Toute modification de la disposition des meubles fait l'objet d'une remise en ordre à la fin du cours.

5.3 (Article 45 du RI Énap) : La médiathèque**5.3.1 (Article 45.1 du RI Énap)**

Les horaires de la médiathèque sont portés à la connaissance des usagers par affichage.

5.3.2 (Article 45.2 du RI Énap)

L'accès à la médiathèque est gratuit pour tous les usagers. Le badge nominatif de l'usager est obligatoire pour obtenir le prêt et la consultation des postes informatiques. Pour ce qui concerne les impressions, les usagers peuvent imprimer dans la limite de 50 feuilles par période de 7 jours. Ils peuvent également imprimer des documents à la Ferme de Trenque ou dans les algécos, sans limitation, sous réserve de fournir eux-mêmes le papier.

Photocopies : les usagers peuvent acheter une carte d'achat de photocopies. Le distributeur de cartes se trouve à la Médiathèque et est disponible aux heures d'ouverture.

5.3.3 (Article 45.3 du RI Énap)

La médiathèque est un lieu consacré à l'étude et la recherche. Aussi chacun adopte une attitude propice à une atmosphère de travail. De même, une tenue vestimentaire correcte est exigée. Il est interdit de faire usage de son téléphone portable et d'introduire dans les locaux des boissons ou nourriture.

5.3.4 (Article 45.4 du RI Énap)

L'accès aux messageries personnelles électroniques n'est pas autorisé, de même que l'utilisation de clé USB.

Article 6 : Les autres structures (Extraits du TITRE 4 : La vie sur le campus)**6.1 (Article 47 du RI Énap) Parkings et déplacements****6.1.1 (Article 47.1 du RI Énap)**

Des parkings sont à la disposition du personnel, des usagers et des passagers. En cas de saturation de ces espaces, les usagers stationnent leur véhicule aux endroits prévus à cet effet dans l'environnement urbain afin de ne occasionner aucune gêne aux riverains ou aux activités commerciales.

6.2 (Article 48 du RI Énap) Structures dédiées à la culture, à la détente et aux loisirs**6.2.1 (Article 48.1 du RI Énap)**

Le personnel et les usagers ont accès, selon les horaires fixés, aux différentes structures de détente et de loisirs de l'école : installations sportives, le foyer dit la ferme de Trenque.

Les usagers peuvent disposer d'espaces pédagogiques pour des temps de rencontres, d'études et de révision en semaine de 17h à 22h, samedi et dimanche, après réservation à l'accueil.

6.2.2 (Article 48.3 du RI Énap)

Toute activité sportive ou autre pratiquée par un résident sur le temps extrascolaire relève de la responsabilité individuelle et de l'assurance civile garantissant les risques liés à ces activités. Les activités relevant de la compétence de l'association des personnels et des élèves (APE) se déroulent principalement au gymnase, aux heures indiquées par leur propre règlement. L'Énap se dégage de toute responsabilité en cas de blessure lors des activités de loisirs qui ne font pas partie des obligations de servir

et ne constituent pas le prolongement normal des fonctions ou de la formation.

6.2.3 Le responsable de formation en charge de la session communique au stagiaire les informations concernant les activités socioculturelles ou sportives organisées par l'unité communication, actions culturelles et événementielles.

Article 7 : La sécurité du site (Extraits du TITRE 5 : La sécurité du site)

7.1 (Article 50 du RI Énap) Accès au site de l'Énap

7.1.1 (Article 50.1 du RI Énap)

Le campus est en accès contrôlé. Pour des raisons de sécurité, certains espaces sont ou seront sous le contrôle d'un dispositif de vidéo protection. Aussi une note de service et des panneaux informeront régulièrement les usagers et les personnels des endroits sous le champ d'une caméra de surveillance au fur et à mesure de leur installation. La direction de l'École établit par note de service les conditions et modalités d'accès au sein du campus de l'École.

7.1.2 (Article 50.2 du RI Énap)

L'accès des locaux de l'école est interdit à toute personne ne bénéficiant pas d'une autorisation temporaire ou permanente délivrée par la direction. Sauf autorisation de la direction, l'introduction et la détention d'armes, hors dotation administrative, des catégories A, B, C et D, réelles ou factices, par toute personne pénétrant sur le campus est interdite.

7.1.3 (Article 50.3 du RI Énap)

La médiathèque de l'école bénéficie d'un libre accès pour toutes les personnes ayant accès à l'Énap. Les personnes étrangères à l'administration pénitentiaire ont un accès préalablement autorisé par les responsables du service.

7.2 (Article 51 du RI Énap) Port du badge

7.2.1 (Article 51.1 du RI Énap)

Pendant leur séjour, les élèves sont dotés d'un badge nominatif avec photo, les stagiaires sont porteurs de leur carte professionnelle et les visiteurs d'un badge de couleur. Le personnel permanent de l'Énap est également soumis au port du badge selon les modalités établies par la note de service du 20 septembre 2016.

7.2.2 (Article 51.2 du RI Énap)

Le badge est nominatif et il doit être présenté lors d'un contrôle par un personnel de sécurité. Toute perte ou détérioration de badge est signalée sans délai. La fabrication d'un nouveau badge est facturée selon les modalités mises en œuvre par le secrétariat général.

Article 8 : Santé et sécurité (Extraits du TITRE 7 : La santé et la sécurité au travail)

8.1 (Article 61 du RI Énap) Prévention d'accidents

8.1.1 (Article 61.1 du RI Énap)

Dans le cadre de la prévention des accidents, chaque personnel et usager prend connaissance des consignes de sécurité affichées dans les locaux et accessibles sur un réseau partagé. La responsabilité disciplinaire peut être engagée pour l'inobservation de ces instructions.

8.1.2 (Article 61.2 du RI Énap)

Chaque personnel, ou usager veille à sa sécurité personnelle et à celle des autres. Il s'abstient de toute imprudence et de tout désordre nuisant à la sécurité d'autrui. Tout risque direct de danger est porté à la connaissance de la direction.

8.1.3 (Article 61.3 du RI Énap)

Tout accident survenu soit pendant le trajet entre le lieu de travail et le domicile, soit au cours du travail, est immédiatement porté à la connaissance du supérieur hiérarchique par le personnel ou l'utilisateur ou par un témoin, sauf cas de force majeure ou impossibilité absolue.

Les registres Hygiène et Sécurité sur lesquels sont portées les

remarques des personnels et usagers peuvent être renseignés dans les lieux désignés par note de service.

8.1.4 (Article 61.4 du RI Énap)

La reconnaissance d'accident de service par la direction de l'école doit avoir un lien de causalité avec l'exécution des fonctions de l'élève. Par conséquent, sera reconnu comme accident imputable au service tout accident survenu dans l'exercice ou à l'occasion de l'exercice de ses fonctions au cours d'une activité qui constitue le prolongement du service.

8.2 (Article 64 du RI Énap) Prévention sanitaire

8.2.1 (Article 64.1 du RI Énap)

Des crises sanitaires épidémiques ou pandémiques peuvent modifier temporairement ou durablement les mesures sanitaires à respecter au sein de l'École.

L'épidémie est définie par l'OMS comme la propagation à l'échelle locale, nationale ou sous-continentale d'une maladie.

La pandémie est définie comme une propagation mondiale de cette même maladie.

Pour le territoire français, le Gouvernement et les autorités sanitaires étatiques sont seuls compétents pour estimer que tout ou partie du territoire est concerné par une épidémie ou une pandémie.

8.2.2 (Article 64.2 du RI Énap)

En cas d'épidémie ou de pandémie, le directeur de l'École édicte les mesures en vigueur au sein de l'établissement par une note circonstanciée afin de garantir la sécurité sanitaire sur le site en faisant appliquer les directives générales des autorités nationales et en les adaptant à la configuration de l'École. Ces mesures s'appliquent à toute personne présente sur le site.

8.2.3 (Article 64.3 du RI Énap)

Les personnels, élèves et stagiaires sont tenus de respecter les consignes sanitaires imposées en cas d'épidémie ou de pandémie sous peine de se voir appliquer une procédure disciplinaire, prévue à l'article 58 du RI Énap (repris dans l'article 10.2 de ce règlement).

Ces consignes sont définies par les autorités sanitaires étatiques compétentes.

8.2.4 (Article 64.4 du RI Énap)

En période d'épidémie ou de pandémie active, les personnels, élèves et stagiaires sont tenus de respecter certaines modalités sanitaires spécifiques liées à l'organisation du travail au sein de l'École. Ces consignes particulières sont définies par la direction de l'École.

8.2.5 (Article 64.5 du RI Énap)

Les personnels, élèves et stagiaires sont invités à informer le service des ressources humaines ou les unités de formation d'un résultat de dépistage médical positif les concernant.

Article 9 : Représentation des stagiaires (selon les dispositions des articles R6352-9 à R6352-14 du code du travail)

Les dispositions des articles du code du travail susmentionnées dans l'article 9 ne concernent que les actions de formation d'une durée totale supérieure à 500 heures.

Article 10 : Discipline (Extraits du TITRE 6 – La discipline et selon les dispositions des articles R6352-3 à R6352-8 du code du travail)

10.1 (Article 57 du RI Énap) L'utilisation des moyens de communication et réseaux sociaux

10.1.1 (Article 57.1 du RI Énap)

Comme tous les citoyens, les usagers et personnels peuvent s'exprimer librement sur les réseaux sociaux dans la limite du respect des obligations de réserve, discrétion et secret professionnel auxquelles ils sont tenus.

10.1.2 (Article 57.2 du RI Énap)

Les commentaires sur les réseaux sociaux de nature à dégrader l'image de l'administration, à déclencher des situations de risques psychosociaux, à livrer des informations liées à la sécurité

pénitentiaire, entraînent une demande écrite d'explications, et peut déclencher l'ouverture d'une procédure disciplinaire à l'encontre du divulgateur.

10.1.3 (Article 57.3 du RI Énap)

L'utilisation des ordinateurs et /ou des réseaux mis à disposition du personnel et des usagers fait l'objet d'une charte d'utilisation dont le respect doit être constant.

10.1.4 (Article 57.4 du RI Énap)

L'usage à titre personnel des téléphones portables est interdit durant les heures de cours. En revanche, son utilisation ou celle d'autres supports et moyens informatiques destinés à l'acquisition des connaissances et prise de notes est autorisée pendant le temps pédagogique.

10.1.5 (Article 57.5 du RI Énap)

L'enregistrement audio, vidéo ou photographique est interdit durant les cours sans autorisation préalable du formateur.

10.1.6 (Article 57.5 du RI Énap)

L'ensemble des personnes accédant aux ressources du système d'information de l'Énap est soumis à la charte régissant l'usage des ressources du système d'information de l'Énap, ainsi qu'à la politique de gestion des journaux d'informatique de l'École. Ces chartes sont annexées au présent règlement intérieur. Le non respect de ces chartes peut entraîner la mise en œuvre de poursuites disciplinaires, voire judiciaires le cas échéant.

10.2 (Article 58 du RI Énap) Procédure disciplinaire

10.2.1 (Article 58.1 du RI Énap)

La finalité des obligations des personnels ou des usagers est de se placer au service de l'intérêt général. Il est donc essentiel que soient respectés les devoirs et obligations conformément à la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, à la loi n°84-16 du 11 janvier 1984 portant dispositions relatives à la fonction publique de l'État, à l'ordonnance n°58-696 du 06 août 1958 et au décret n°66-874 du 21 novembre 1966 relatifs au statut spécial des personnels des services déconcentrés de l'administration pénitentiaire, au décret n° 94-874 du 07 octobre 1994 fixant les dispositions communes applicables aux stagiaires de l'État et des établissements publics, au décret n° 2000-1328 modifié du 26 décembre 2000 relatif à l'Énap, et au décret n°2016-547 du 03 mai 2016 modifiant le décret n°2000-1328 du 26 décembre 2000.

10.2.2 (Article 58.2 du RI Énap)

La faute s'analyse de manière concrète à partir du comportement de l'agent vis-à-vis de l'administration, des administrés et des obligations auxquelles il est tenu dans le cadre de ses fonctions.

10.2.3 (R6352-3 du code du travail) Constitue une sanction toute mesure, autre que les observations verbales, prise par le directeur de l'organisme de formation ou son représentant, à la suite d'un agissement du stagiaire considéré par lui 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 amendes ou autres sanctions pécuniaires sont interdites.

10.2.4 (Article 58.3 du RI Énap)

Des demandes d'explications peuvent être rédigées par tout personnel en position hiérarchique, s'agissant du personnel de l'école, par le cadre désigné par la direction ; s'agissant des usagers, par les responsables des unités de formation sous l'autorité de la direction de la formation. Elles sont ensuite transmises à la direction de l'école pour les suites à donner.

10.2.5 (R6352-4 du code du travail) Aucune sanction ne peut être infligée au stagiaire sans que celui-ci ait été informé au préalable des griefs retenus contre lui.

10.2.6 (R6352-5 du code du travail) Lorsque le directeur de l'organisme de formation ou son représentant envisage de prendre une sanction qui a une incidence, immédiate ou non, sur la présence d'un stagiaire dans une formation, il est procédé comme suit : 1° Le directeur ou son représentant convoque le stagiaire en lui indiquant l'objet de cette convocation. Celle-ci précise la date, l'heure et le lieu de l'entretien. Elle est écrite et est adressée par lettre recommandée ou remise à l'intéressé contre décharge ; 2° Au cours de l'entretien, le stagiaire peut se faire assister par la personne de son choix, notamment le délégué de

stage. La convocation mentionnée au 1° fait état de cette faculté ; 3° Le directeur ou son représentant indique le motif de la sanction envisagée et recueille les explications du stagiaire.

10.2.7 (Article 58.4 du RI Énap)

Après la commission d'une faute grave, la direction de l'école peut, à l'issue d'un entretien avec le contrevenant, décider d'une interdiction conservatoire de suivre la formation, de se rendre sur le site de l'école ou des stages, le temps de l'instruction de la procédure disciplinaire. Cette interdiction n'emporte pas suspension du traitement.

10.2.8 (R6352-7 du code du travail) Lorsque l'agissement a rendu indispensable une mesure conservatoire d'exclusion temporaire à effet immédiat, aucune sanction définitive, relative à cet agissement, ne peut être prise sans que la procédure prévue à l'article R. 6352-4 et, éventuellement, aux articles R. 6352-5 et R. 6352-6, ait été observée.

10.2.9 (Article 58.5 du RI Énap)

L'avertissement (sans inscription au dossier), ou le blâme peut être prononcé par la direction de l'école après avoir entendu ou fait entendre un élève, un stagiaire, un auditeur. L'intéressé peut se faire assister d'une personne de son choix à l'occasion de cet entretien.

10.2.10 (R6352-8 du code du travail) Le directeur de l'organisme de formation informe l'employeur et l'organisme financeur de la sanction prise.

10.3 (Article 60 du RI Énap) Responsabilités

10.3.1 (Article 60.1 du RI Énap)

Les usagers sont responsables disciplinairement et pécuniairement des dégâts qu'ils commettent volontairement ou lorsqu'ils contreviennent aux consignes données, au détriment des biens mis à leur disposition à l'école ou sur les lieux de stages. Ils sont responsables pécuniairement des pertes concernant les objets ou effets confiés à leur soin.

10.3.2 (Article 60.2 du RI Énap)

La procédure de recouvrement éventuel des sommes dues sera initiée par le secrétaire général de l'Énap et mise en œuvre par l'agent comptable, après signature d'une convention transactionnelle ou par le moyen de l'assurance personnelle de l'intéressé.

10.3.3 (Article 60.3 du RI Énap)

L'école ou son personnel ne peut être tenu pour responsable de la perte, disparition ou dégradation d'objets de valeur apportés ou portés par un personnel ou un usager sauf circonstances exceptionnelles.

Article 77 : Transmission du règlement

Un exemplaire du règlement applicable aux stagiaires de la formation professionnelle proposée par l'Énap, organisme de formation, est transmis par messagerie électronique à chaque stagiaire (avant toute inscription définitive).

Article 78 : Application du règlement

La direction de l'Énap est chargée de l'exécution du présent règlement.

Tout manquement aux obligations de ce règlement intérieur peut entraîner le dépôt d'une demande d'explication préalable à une éventuelle procédure disciplinaire.

Sophie BONDIL
Directrice de l'Énap



ANNEXES



CHARTE RÉGISSANT L'USAGE DES RESSOURCES

du SYSTÈME D'INFORMATION de l'Énap

Février 2023

Table des matières

1. ACRONYMES ET DEFINITIONS	4
1.1 Acronymes	4
Définitions	4
2. PRESENTATION	7
2.1 Objet	7
2.2 Domaine d'application	7
2.3 Engagements de l'Énap	7
2.4 Engagement de l'utilisateur	8
3. CONDITIONS ET REGLES D'UTILISATION DES RESSOURCES DU SYSTEME D'INFORMATION	8
3.1 Accès et utilisation des ressources du système d'information	8
3.2 Droit à la déconnexion	9
3.3 Utilisation d'équipements (ordinateur, mobile, tablette) externes au système d'information de l'Énap (privés ou extérieurs) dans le cadre professionnel	9
3.4 Utilisation d'objets connectés	9
3.5 Utilisation des ressources informatiques	9
3.5.1 Usage interne à l'Énap	9
3.5.2 Usage externe à l'Énap	10
3.6 Utilisation des ressources à titre privé	11
3.7 Modalités relatives au Télétravail	11
3.8 Utilisation des logiciels, applications et base de données	12
3.9 Utilisation des services numériques du ministère de la Justice	12
3.10 Traitement des données à caractère personnel	13
3.11 Données particulières ou sensibles	13
3.11.1 Stockage des données sensibles	13
3.11.2 Traitement des données sensibles	14
3.11.3 Transfert de données sensibles	14
3.11.4 Transfert de données classifiées	14
3.12 Traitement à caractère personnel n'ayant pas fait l'objet d'un accord préalable.	14
4. UTILISATION D'INTERNET	14
4.1 Accès à Internet	14
4.1.1 Téléchargement ou transfert de fichiers	15

4.2	Utilisation du réseau privé virtuel Justice (Intranet Justice)	15
5.	COMMUNICATIONS ELECTRONIQUES	15
5.1	Adresses électroniques	15
5.2	Contenu des messages électroniques.....	16
5.3	Émission et réception de messages.....	16
5.4	Émission de messages comportant des données à caractère personnel	16
5.5	Statut et valeur juridique des messages	17
5.6	Stockage et archivage des messages.....	17
5.7	Messagerie instantanée et réseaux sociaux.	17
6.	CONTINUE DE SERVICE.....	17
6.1	Devoir de signalement et d'information.....	17
7.	EXPLOITATION ET CONTROLE	18
7.1	Les ressources du système d'information.....	18
7.2	Autres moyens de télécommunications	18
8.	TRAÇABILITE.....	18
9.	LOIS ET REGLEMENTATIONS APPLICABLES.....	19
9.1	Propriété intellectuelle.....	19
9.2	Réglementation à l'égard de traitement des données à caractère personnel	19
9.3	Traitement de données à caractère personnel non déclaré.....	19
9.4	Droits des personnes concernées	20
9.5	Politique de Sécurité des Systèmes d'Information de l'Etat.....	20
9.6	Protection du secret de la défense nationale et protection des systèmes d'informations sensibles	20
9.7	Protection du potentiel scientifique et technique de la nation.....	20
9.8	Autres lois et réglementations applicables (liste non exhaustive).....	21
10.	SANCTIONS.....	21
11.	DUREE DE VALIDITE ET REVISION DE LA CHARTE	22
12.	ENTREE EN VIGUEUR DE LA CHARTE	22

1. Acronymes et définitions

1.1 Acronymes

Pour faciliter la lecture de ce document la charte utilise divers acronymes listés ci-après :

Énap	Ecole Nationale d'Administration Pénitentiaire
AP	Administration Pénitentiaire
DPD	Délégué à la Protection des Données
RT	Responsable de Traitement
RSSI	Responsable de la Sécurité des Systèmes d'Information
DSI	Département des Systèmes d'information
RGPD	Règlement Général sur la Protection des Données
LIL	Loi Informatique et Libertés
RPVJ	Réseau Privé Virtuel Justice
SI	Système d'Information

Définitions

Activités de l'Énap	L'activité de l'Énap est celle découlant des missions définies par le code pénitentiaire (articles R112-43 R 112-66), à savoir : 1° La formation professionnelle initiale et tout au long de la vie des fonctionnaires et agents publics occupant un emploi dans l'administration pénitentiaire ainsi que la formation professionnelle continue des partenaires du service public pénitentiaire ; 2° La préparation à des concours de la fonction publique et, à ce titre, organise des préparations destinées à permettre la diversification des recrutements, dont les modalités sont définies par arrêté du garde des sceaux, ministre de la justice ; 3° La réalisation de travaux de recherches et d'études et leur diffusion ; 4° Le développement et la mise en œuvre d'actions de partenariat avec des institutions d'enseignement et de recherche ; 5° Le développement et la mise en œuvre d'actions de coopération internationale, notamment en matière de formation et de recherche, mais également toute activité administrative et de gestion découlant de ses activités.
Code ou logiciel malveillant	Désigne un code ou logiciel développé dans le but de nuire aux ressources d'un SI. Les virus, vers, chevaux de Troie ou bombes logiques constituent des exemples de <i>codes ou de logiciels malveillants</i> .
Traitement de données à caractère personnel	Désigne toute opération ou ensemble d'opérations portant sur des données à caractère personnel, quel que soit le procédé utilisé telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.
Responsable du traitement	Désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ;

Accès applicatif	Désigne la journalisation de toute connexion à un applicatif ainsi que le traçage de l'utilisateur dans l'utilisation de l'applicatif. Cette journalisation est utilisée uniquement dans les traitements comportant des données à caractère personnel ou relevant d'une obligation légale (Internet).
Entité	Désigne toutes les entités existantes au sein de l'Énap, à travers ses composantes et services pour l'accomplissement de ses missions. Exemples : départements d'enseignement, filières de formation, services administratifs ; techniques, département de la recherche, département formation renseignement pénitentiaire...
Messagerie	La messagerie électronique comprend les systèmes de courrier électronique, de messagerie instantanée et messagerie texte (SMS).
Apprenants	Toutes personnes suivant en présentiel ou en distanciel une formation ou action de formation en lien l'Énap.
Personne juridiquement responsable	Toute personne ayant la capacité de représenter l'Énap (directeur de l'Énap, directeur adjoint et toutes personnes disposant d'une délégation de pouvoir).
Responsable de la Sécurité des Systèmes d'Information (RSSI)	Désigne la personne responsable sécurité informatique qui évalue la vulnérabilité du système d'information de l'Énap, il définit et met en œuvre la politique de sécurité de l'Énap. Il met en place des solutions pour garantir la disponibilité, la sécurité et l'intégrité de système d'information et des données.
Délégué à la protection des données (DPD)	Désigne la personne en charge de la protection des données à caractère personnel, il conseille et informe le responsable de traitement. Il est le point de contact avec l'autorité de contrôle (Cnil).
Réseau Justice ou Intranet Justice	Désigne la mise à disposition et l'accès aux ressources et services proposés par le ministère de la Justice sur le réseau privé virtuel Justice ainsi que par extension toutes les connexions offertes sur les autres réseaux privés provenant d'autres ministères et utilisant l'intranet Justice comme moyen d'accès (Minefi, Maya ...).
Services Internet	Désigne la mise à disposition par des serveurs, locaux ou distants, de moyens d'échanges et d'informations diverses (Moodle Énap, Office 365, TEAMS, Catalogue médiathèque ...)
Responsable de l'utilisateur	Le responsable de l'utilisateur est : Pour les agents titulaires ou non titulaires concourant à l'exécution des missions du service public de l'Énap : le responsable de la direction ; Pour les apprenants : le directeur de la formation, le directeur de l'Énap ou son adjoint ; Pour les prestataires : le responsable interne à l'Énap du contrat de prestation ou de la convention ; Pour les partenaires internes à la Justice ou externe le directeur de l'Énap ou son adjoint ;
Ressources du Système d'information (S.I.)	Ensemble des ressources techniques, applicatives, organisationnelles, humaines et documentaires permettant d'accéder, collecter, stocker, traiter, détruire, rechercher et/ou transmettre des données, en particulier : Tout matériel informatique fixe : postes (dont les postes libre-service), serveurs, téléphones, périphériques (clavier, écran, imprimante, photocopieur intelligent, etc.), prises, câbles, ... Tout matériel informatique mobile : ordinateur, téléphone, etc. Tout logiciel ou service réseau ou informatique : accès réseau, accès Internet, messagerie électronique, bureautique, etc. Tout support de données : électronique, papier, etc. Le réseau Justice (RPVJ) et les services Internet offert par l'Énap
VPN-Énap	Désigne un moyen technique offert par l'Énap permettant d'accéder aux ressources du système d'information de l'Énap de manière sécurisée (utilisé pour le télétravail). Appelé aussi communément Systancia sur l'Énap.

Télétravail	L'article L 1222-9 du code du travail dispose que « (...) le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication (...) ».
Utilisateur	Toute personne / individu ayant accès ou utilisant les ressources du système d'information de l'Énap, quel que soit son statut, en particulier : Tout agent titulaire ou non-titulaire concourant à l'exécution des missions du service public de l'Énap (fonctionnaire, contractuel ou vacataire) ; Tout agent du ministère de la Justice accédant à des traitements de données à caractère personnel hébergé par l'Énap. (Violette, Iris) Tout formateur occasionnel justice ou extérieur, utilisant les ressources de l'Énap, y compris les locaux et le matériel ; Tout élève, stagiaire en formation initiale d'adaptation ou continue ; Tout prestataire sous contrat ou convention avec l'Énap ; Tout stagiaire (hors AP) utilisant les ressources de l'Énap, y compris les locaux ; Tout lecteur autorisé qui dispose d'un accès aux ressources bibliographiques en ligne ; Toute personne accédant à un service hébergé par l'Énap, y compris le site internet et les services Moodle et OFFICE 365 ; Toute personne accueillie temporairement au sein de l'Énap et ayant de ce fait accès à un poste informatique de l'Énap et/ou au réseau informatique (formateur externe, conférencier, intervenant pédagogique ou technique, invité, etc.). Tout apprenti, stagiaire effectuant un stage de formation Tout visiteur

2. Présentation

2.1 Objet

L'objet de la présente charte est d'informer les utilisateurs des ressources du système d'information de l'Énap de leurs droits et obligations.

Elle est associée à la charte d'usage des services numériques du ministère de la Justice, et aux différentes chartes propres à l'utilisation de services internes spécifiques proposés par l'Énap (Office 365, Télétravail, MOODÉnap...).

Chaque utilisateur doit être conscient de l'impact de son usage quotidien ou occasionnel sur la sécurité des ressources du système d'information, et s'engage à accepter cette charte dans tous ses éléments et à la respecter dans tous ses termes.

2.2 Domaine d'application

Les règles et obligations énoncées dans la présente charte s'appliquent à tout utilisateur des ressources du système d'information de l'Énap.

A ce titre, la présente charte doit être communiquée à tout utilisateur interne ou extérieur de l'Énap utilisant ces ressources informatiques. La charte est diffusée à l'ensemble des utilisateurs et mise à disposition sur le panneau d'affichage de l'Énap des salles informatiques, ainsi que sur son intranet.

Des exemplaires sont disponibles auprès du service de l'Accueil.

Les contrats souscrits entre l'Énap et tous tiers donnant accès aux données, aux programmes informatiques ou à tout autre moyen de l'Énap devront stipuler que ces utilisateurs s'engagent à respecter la présente charte.

L'Énap en tant que commanditaire définira contractuellement (contrat, marché public...) les autorisations et dispositions nécessaires à l'accomplissement de la prestation.

Les personnels de l'Énap faisant appel à des prestataires extérieurs s'engagent à faire respecter la présente charte.

Les ressources du système d'information comprennent les serveurs, les stations de travail, les ordinateurs portables, les équipements réseaux, les équipements mobiles, les smartphones ou ordiphones, les supports de stockages amovibles (clé USB, disque dur, CD ou DVD) et tous types de périphériques situés dans les services administratifs, les locaux d'enseignement, la médiathèque, les hébergements et tout autre local de l'Énap disposant de tels matériels présents dans les locaux de l'Énap ou à l'extérieur de ceux-ci.

Cette charte impacte aussi, les installations de l'Énap permettant de se connecter ou de dialoguer avec des sites informatiques dans le monde entier.

Les règles définies par la présente charte s'étendent également à l'utilisation des ressources et des réseaux extérieurs, accessibles par l'intermédiaire de réseaux d'interconnexion comme internet ou par l'utilisation du VPN Énap (télétravail).

L'utilisation de l'Intranet Justice et de ces dépendances est subordonnées à la signature et l'acceptation de la charte d'usage des services numériques du ministère de la Justice.

2.3 Engagements de l'Énap

L'Énap porte à la connaissance des utilisateurs la présente charte ainsi que la charte d'usage des services numériques du ministère de la Justice.

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

L'Énap facilite l'accès des utilisateurs aux ressources du système d'information.

Les ressources mises à leur disposition sont prioritairement à usage professionnel, mais l'Énap est tenue de respecter l'utilisation du système d'information à titre privé.

L'utilisation à des fins privées des services et ressources numériques est tolérée dans la limite des nécessités de la vie courante et familiale.

Cet usage à titre extra-professionnel doit être mesuré et ne peut en aucun cas se faire au détriment des tâches ou missions professionnelles incombant à l'utilisateur. Il ne doit en aucun cas nuire au bon fonctionnement de l'ensemble des ressources numériques de l'Énap ou altérer son image.

2.4 Engagement de l'utilisateur

L'utilisateur est responsable, en tout lieu et en tout temps, de l'usage qu'il fait des ressources du système d'information de l'Énap.

L'utilisateur s'engage à respecter les dispositions de la présente charte.

Le non-respect des règles de bonne conduite énoncées dans la présente charte et ses annexes engage la responsabilité personnelle de l'utilisateur.

3. Conditions et règles d'utilisation des ressources du système d'information.

3.1 Accès et utilisation des ressources du système d'information

L'utilisation des ressources du système d'information de l'Énap et la connexion d'un équipement externe au système d'information sont soumises à autorisation.

L'utilisateur est informé que :

- Ses codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation proscribed ou malveillante des ressources du système d'information ;
- Ses accès sont définis par l'Énap en fonction de son statut ;
- Chaque utilisateur peut se voir attribuer un ou plusieurs codes d'accès aux ressources du système d'information. Ces codes d'accès sont constitués d'un identifiant unique et nominatif attribué par l'Énap et d'un mot de passe choisi par l'utilisateur. Lors de la création d'un compte ou accès, si le DSI a généré un mot de passe automatique, l'utilisateur a pour obligation de le changer lors de sa première connexion et le plus rapidement possible.
- Le mot de passe est le garant de votre identité numérique, en aucun cas il ne doit être révélé, ni au DSI, ni à votre supérieur hiérarchique. En cas de vacance de poste et sur instruction du directeur de l'Énap, le DSI pourra créer de nouvelles habilitations permettant l'accès aux ressources visées.

Afin d'assurer la sécurité des accès aux ressources du système d'information, l'utilisateur doit :

- Garder strictement confidentiel(s) son (ses) code(s) d'accès et ne pas le(s) dévoiler à un tiers. L'utilisateur est responsable de l'utilisation qui est faite de ses codes d'accès, leur divulgation volontaire à un tiers engage sa responsabilité pénale et civile ;
- Respecter les règles en vigueur au sein de l'Énap concernant les mots de passe ;
- Respecter les consignes de sécurité et les règles relatives aux codes d'accès, en particulier :
 - Ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître ;
 - S'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information en contournant les droits attribués ;
 - Ne pas connecter directement au système d'information des matériels autres que ceux confiés ou autorisés par l'Énap.
 - Utiliser un code d'accès fort comprenant au moins 8 caractères de trois types, (majuscule, minuscule, chiffre ou caractère spécial).
- S'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources du système d'information, que ce soit par des manipulations anormales du matériel (par exemple, débrancher un câble réseau), ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, logiciels d'écoute réseau, etc.

Afin d'assurer la sécurité des accès aux ressources du système d'information, l'Énap est tenue de :

- Veiller à ce que les ressources ne soient accessibles qu'aux personnes habilitées ;
- Supprimer, désactiver ou modifier les codes d'accès dès que la situation le justifie : fin de l'activité de l'utilisateur, longue période de vacance de poste, non-respect de la charte, etc.

Pour les accès distants aux ressources du système d'information, il est rappelé que les chartes des différents fournisseurs d'accès au réseau Internet empruntés par l'utilisateur s'appliquent (Intranet Justice).

Enfin, l'utilisateur doit restituer tout matériel informatique et de télécommunication confié par l'Énap (poste de travail portable, téléphone mobile...) lorsqu'il quitte définitivement ses fonctions (retraite, démission, ...) ou lorsqu'il change d'affectation (en dehors ou au sein du ministère).

3.2 Droit à la déconnexion

Il convient de respecter les périodes de congés ou d'interruption du travail durant lesquelles les agents ne sont pas censés répondre aux [sollicitations](#) de leur employeur.

Au demeurant, ces sollicitations ne peuvent se justifier qu'en raison des nécessités de services pour faire face à une situation d'urgence (à apprécier selon les fonctions exercées).

L'usage de la messagerie électronique ou du téléphone, en dehors des horaires de travail, doit se faire en respectant la vie privée du destinataire et de l'émetteur ainsi que le droit à la déconnexion du destinataire et de l'émetteur, sauf pour faire face à une situation d'urgence.

3.3 Utilisation d'équipements (ordinateur, mobile, tablette) externes au système d'information de l'Énap (privés ou extérieurs) dans le cadre professionnel

De manière générale seuls les matériels fournis, configurés et gérés par l'Énap (ou le ministère de la justice) sont autorisés à être connectés au **réseau filaire ou Ethernet** de l'Énap.

Toutefois, pour répondre à la nécessité de service, l'utilisation d'un équipement externe dans le cadre d'activités professionnelles pourra être autorisée sous conditions :

- L'utilisateur s'engage à utiliser cet équipement uniquement à but professionnel
- L'utilisateur doit avoir reçu l'autorisation écrite du RSSI de l'Énap après demande motivée du responsable du chef de département. Le RSSI donnera à cette occasion les prérequis à l'utilisation de ce matériel.
- L'Énap ne peut être tenue responsable d'éventuels vols ou endommagements du matériel ni en cas de pertes de données personnelles.

L'autorisation d'utilisation du réseau Wifi de l'Énap est subordonnée à l'utilisation d'un couple login/ mot de passe personnel.

Ces accès sont strictement individuels et confidentiels, ils ne peuvent être cédés comme il est mentionné dans la section 3.1 de la présente charte.

L'utilisation du réseau Wifi dans l'enceinte de l'Énap est soumise aux conditions de la présente charte.

3.4 Utilisation d'objets connectés

Les objets connectés personnels (smartphones, écouteurs sans fil, montres, etc.) utilisés à titre privé ne doivent pas être branchés aux équipements professionnels.

Toute connexion de ces objets sur le matériel informatique ou téléphonique de l'Énap, même éteints, est prohibée (pas de recharge via une connexion USB, pas de partage de données).

L'utilisation de ces appareils doit être restreinte afin d'éviter tous risques de captation d'informations.

L'introduction d'objet connecté au sein du département de formation du renseignement pénitentiaire est strictement interdite.

3.5 Utilisation des ressources informatiques

3.5.1 Usage interne à l'Énap

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe le service informatique de toute anomalie constatée.

Chaque utilisateur s'engage à ne pas déplacer ni à débrancher le matériel informatique mis à disposition dans les locaux pédagogiques ou administratifs.

L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire et d'utiliser de façon optimale les moyens de compression des fichiers dont il dispose.

L'utilisation des ressources informatiques doit être rationnelle et loyale afin d'en éviter la saturation.

Toute ressource informatique propre à un département, unité, de l'Énap, doit être connectée au réseau par un technicien informatique de l'ÉNAP. Ce dernier s'assure en particulier que les règles de sécurité en vigueur sont bien respectées.

Un utilisateur ne doit jamais quitter son poste de travail personnel ou en libre-service sans se déconnecter.

3.5.2 Usage externe à l'Énap

3.5.2.1 Ordinateur et smartphone ou ordiphone

Le matériel informatique et de télécommunication que l'Énap fournit est placé sous la responsabilité de l'utilisateur, en tous lieux et en toute circonstance.

Lors de l'utilisation d'équipements nomades ou mobiles (notamment lors de voyages, déplacements, télétravail), les risques de compromission potentielle de l'information sont plus élevés.

À ce titre, l'utilisateur doit utiliser les moyens de protection mis à sa disposition (câble antivol, armoire sécurisée, etc.) et appliquer les consignes de sécurité (verrouillage de l'ordinateur) afin de se prémunir contre le vol d'information.

Il doit aussi assurer la confidentialité des informations traités en s'assurant que celles-ci ne soient pas exposées à la vue d'autrui, l'utilisation d'un filtre de confidentialité est fortement recommandée en cas d'usage dans les lieux ou transports publics.

3.5.2.2 Stockage externe

L'utilisateur doit faire preuve d'une attention particulière lors de l'emploi des supports amovibles de stockage de masse (tels clés USB, disques durs externes, ...) et limiter autant que possible les supports non fournis par l'Énap. En effet, ces supports peuvent être porteurs de programmes malveillants.

Ainsi, il ne doit pas connecter sur ses équipements informatiques des supports amovibles provenant de l'extérieur de l'Énap sans faire vérifier la sécurité de leurs matériels amovibles auprès du DSI de l'Énap.

Toute connexion d'un support de masse fourni ou non par l'Énap sur un ordinateur ou système d'information extérieur, entraîne de facto l'obligation d'une vérification par le DSI ou par les stations blanches situées au sein de l'Énap.

3.5.2.3 Missions à l'étranger

L'attention de l'utilisateur est appelée sur l'emploi des ressources du système d'information en mobilité qui présente des risques plus élevés et des conséquences plus importantes, notamment lors des déplacements à l'étranger, compte-tenu des formalités douanières de certains pays étrangers (Etats-Unis et Chine en particulier).

Pour éviter toute captation d'information par les autorités douanières, l'utilisateur veille à emporter avec lui uniquement le matériel professionnel et la quantité d'information utiles à sa mission.

L'utilisateur avant son départ devra prendre attache auprès du DSI pour vérifier que son matériel est configuré pour la mission et se voir rappeler les règles édictées et mises à jour par l'ANSSI et les autorités françaises.

En cas d'interception par les autorités douanières, l'utilisateur doit signaler l'incident dans les plus brefs délais à son responsable hiérarchique et au DSI de l'Énap, qui lui indiquera la procédure à suivre.

3.5.2.4 Connexion réseau

La connexion réseau à des réseaux publics (hôtels, gares, magasins...) est proscrite afin de limiter les risques de compromissions. En voyage ou déplacement, l'utilisateur devra se connecter à un réseau Justice identifié ou utiliser la connexion téléphonique « 4G » ou « 5G » du smartphone qui lui est fourni par l'Énap.

3.5.2.5 Perte ou vol

L'utilisateur doit donc faire preuve d'une vigilance accrue pour en assurer la surveillance. En cas de perte ou de vol d'un matériel informatique, de communication ou de support amovible de stockage, il doit **le signaler dans les plus brefs délais** à son responsable hiérarchique et au DSI de l'Énap, qui lui indiquera la procédure à suivre.

3.6 Utilisation des ressources à titre privé

Les ressources du système d'information sont des outils mis à disposition pour une utilisation dans le cadre des activités de l'Énap.

L'utilisation de ces moyens peut également constituer le support d'une communication à titre privé dans les conditions décrites ci-après.

L'utilisation résiduelle des ressources du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service. Toute information est réputée être la propriété de l'Énap à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

L'utilisateur ne doit, en aucun cas transformer et/ou qualifier des données, documents, fichiers ou messages de nature professionnelle en données, documents, fichiers ou messages personnels ou privés.

Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet nommé « PRIVE » ou « PERSONNEL ». La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

Cependant l'Énap procédant à des sauvegardes de manière automatique, il n'est pas fait distinction entre les répertoires et données privés ou personnelles et les données professionnelles.

L'utilisateur, avant son départ définitif de l'Énap, est responsable de la destruction et de la sauvegarde personnelle de son espace de données à caractère privé, la responsabilité de l'Énap quant à la conservation de cet espace ne pouvant être engagée à cet effet.

Au départ définitif de l'utilisateur, ses droits d'accès et habilitations seront suspendus immédiatement.

Ses ayants droits ne seront pas autorisés à accéder aux contenus de l'utilisateur à l'exception des données marquées comme personnelles.

Certaines données sont conservées conformément à la réglementation en vigueur.

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

3.7 Modalités relatives au Télétravail

Le télétravail fait l'objet de modalités définies réglementairement par arrêté du 31 juillet 2019 portant application du décret n°2016-151 du 11 février 2016 modifié et fixant les modalités de mise en œuvre du télétravail au ministère de la Justice et la note d'application du 23 octobre 2020 relative aux conditions et modalités de mise en œuvre du télétravail au ministère de la Justice.

Cette circulaire précise les règles de sécurité informatique à respecter par les agents en télétravail.

L'utilisateur s'engage comme en dispose les articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité et l'intégrité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Tout utilisateur s'engage à suivre une formation au télétravail délivrée par l'Énap et à signer un « *Engagement de sécurité et de confidentialité portant sur l'utilisation des données et des moyens informatiques dans le cadre du télétravail* » avant d'accéder à ce service.

3.8 Utilisation des logiciels, applications et base de données

L'utilisateur ne peut installer aucun logiciel ou composant sur une ressource du système d'information sans l'accord écrit du département des systèmes d'information.

Toute demande de logiciel doit obligatoirement passer par le logiciel Gestionnaire Libre de parc Informatique (GLPI), disponible sur le portail des applications de l'Énap.

L'utilisateur est tenu de :

- Ne pas installer, télécharger ou utiliser volontairement sur le système d'information :
 - Des logiciels non autorisés par l'Énap ou non conformes aux missions de l'Énap ;
 - Des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites de confiance, ou sans autorisation du DSI ;
 - Des versions d'essai ou d'évaluation de logiciels ;
 - Des extensions ou add-on sans autorisation du DSI ;
 - Des codes ou logiciels malveillants
- Ne pas désinstaller, modifier ou empêcher la bonne exécution des logiciels, applications et utilitaires installés sur son poste de travail par le DSI
- Ne pas réaliser des copies de logiciels soumis à licence (exceptées les copies de sauvegarde) ou de mettre à disposition ces logiciels à une tierce personne par l'intermédiaire du réseau ;
- Ne pas contourner les restrictions d'utilisation d'un logiciel autorisé ;
- Respecter les contrats de licence de l'utilisateur final (CLUF)
- Ne pas communiquer ses identifiants, mot de passe (pas de compte générique)
- Signaler rapidement au service informatique tout dysfonctionnement constaté de logiciel, application ou utilitaire installé sur le poste de travail par le service informatique ;
- Respecter la politique de sécurité de l'application ainsi que les règles et procédures en vigueur lors de toute manipulation de données extraites du système d'information.

Lors d'un changement de poste ou d'habilitations d'un utilisateur, le responsable hiérarchique de l'utilisateur concerné a pour obligation d'informer le service compétent conformément à la procédure en vigueur.

3.9 Utilisation des services numériques du ministère de la Justice

L'utilisation des services numériques mises à disposition par le ministère de la Justice est conditionnée à la signature et au respect de la charte d'usage des services numériques du ministère de la Justice.

Les services numériques sont définis comme l'ensemble des processus et des ressources permettant d'acquérir, de générer, de traiter, de stocker, de détruire, de transmettre ou d'accéder à des informations électroniques au sein du ministère de la Justice.

Pour exemple, les logiciels professionnels utilisés dans le cadre de la formation des apprenants ou la gestion administrative des agents entrent dans cette définition.

3.10 Traitement des données à caractère personnel

Tout traitement de données doit être mis en œuvre conformément au règlement général sur la protection des données (RGPD) et la loi dite « Informatique et Libertés ».

A cette intention l'Énap dispose d'un délégué à la protection de données (DPD ou DPO).

Celui-ci doit être saisi pour toute question portant sur des données à caractère personnel et à leurs traitements.

L'utilisateur s'engage à préserver les données à caractère personnel, traitées par l'Énap.

La perte, la destruction, la modification ou la divulgation frauduleuse, accidentelle ou non autorisée de données à caractère personnel doivent faire l'objet **d'une déclaration sans délai** auprès du DPD et de la direction de l'Énap.

L'utilisateur se doit de :

- Informer le DPD préalablement à toute création de fichiers contenant des données à caractère personnel ou traitement sur ces mêmes données, conformément aux dispositions de la loi Informatique et Libertés et du RGPD ;
- faire inscrire son traitement au registre des traitements de l'Énap ;
- le faire valider par la direction de l'Énap ;
- respecter les finalités définies, explicites et légitimes du traitement de données à caractère personnel ;
- protéger les données personnelles afin qu'elles ne soient pas utilisées par des personnes non autorisées ou habilitées, ni divulguées, modifiées, supprimées ou détruites, perdues, volées, même de manière accidentelle (cela suppose le contrôle rigoureux de la diffusion de données à caractère personnel à destination de tiers extérieurs à l'Énap) ;
- lorsqu'un traitement ou application permet la saisie de données dans un champ libre, celles-ci doivent être objectives, non excessives et conformes à la finalité du traitement ;
- respecter et donc ne pas contourner, ni désactiver, les mesures techniques, organisationnelles et juridiques, prises par l'Énap pour assurer la protection des données à caractère personnel.

Les manquements à la réglementation en vigueur peuvent donner lieu à des sanctions à l'encontre de l'Énap de la part de la CNIL.

L'Énap s'est dotée de politiques de confidentialités définissant le cadre et l'utilisation des données à caractère personnel.

3.11 Données particulières ou sensibles

Les données particulières ou sensibles sont les données à caractère personnel au sens des articles 9 et 10 du RGPD et de l'article 30 de la LIL concernant le numéro NIR communément appelé numéro de sécurité sociale.

C'est-à-dire, le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. Ainsi que : Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

L'utilisation, le traitement du NIR ne peut être effectué que pour des finalités dument définies par la réglementation. En aucun cas son utilisation ou conservation ne peut avoir lieu sans consultation préalable du DPD.

Par extension, les données sont considérées comme sensibles si leur divulgation à des personnes non autorisées, leur altération ou leur indisponibilité sont de nature à porter atteinte à la réalisation des missions de l'Énap. Les informations d'authentification (mots de passe, certificats, etc.) sont considérées comme des données sensibles. Les informations stratégiques rentrent dans cette classification.

Tout traitement de ces données doit faire l'objet d'une déclaration préalable auprès du DPD et du RSSI de l'Énap avant sa mise en œuvre.

3.11.1 Stockage des données sensibles

L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire.

L'utilisation de solution externe type cloud ou informatique dans le nuage est totalement proscrite.

L'utilisation de messagerie ou autre moyen de communication non validé par l'Énap est proscrit pour ces données.

Les données sensibles doivent être stockées sur un espace ou matériel dédié à cet usage.

Cet espace ou matériel aura fait l'objet d'une approbation par le DSI.

3.11.2 *Traitement des données sensibles*

Le traitement d'informations sensibles au sein des zones d'accueil est à éviter. Si un tel traitement est strictement nécessaire, il doit rester ponctuel et exceptionnel.

Pour les postes de travail nomades manipulant des données sensibles :

- tous les supports de stockage interne ou externe doivent être cryptés par le DSI,
- un filtre de confidentialité doit être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité ou en présence de tiers non habilité.

3.11.3 *Transfert de données sensibles*

Tout transfert par réseau de données sensibles ou particulières doit faire l'objet d'un protocole écrit et approuvé par le RSSI ou le DPD.

Dans le cas de transfert nécessitant un support physique, le RSSI ou le DPD fournira une solution auprès de l'utilisateur après avoir défini avec lui le niveau de sensibilité des données.

3.11.4 *Transfert de données classifiées*

En ce qui concerne l'échange de données classifiées « Confidentiel Défense » ou « Secret Défense », l'utilisateur doit se conformer aux dispositions prévues dans le cadre de l'Instruction Générale Interministérielle n°1300 du 23 juillet 2010 relative à la protection du secret de la défense nationale.

Seul le personnel habilité peut valider le transfert.

Le RSSI ou le DPD peuvent apporter leur concours dans la mise en place de solutions.

3.12 **Traitement à caractère personnel n'ayant pas fait l'objet d'un accord préalable.**

Tout traitement de données à caractère personnel n'ayant pas fait l'objet d'une inscription aux registres des traitements de l'Énap et ayant reçu l'accord écrit du délégué à la protection des données ou du responsable de traitement sera considérée comme illégale.

La responsabilité de l'Énap ou de son directeur ne pourra être engagée.

Le commanditaire, l'utilisateur du traitement engagera de facto sa responsabilité civile et pénale personnelle.

4. Utilisation d'Internet

4.1 **Accès à Internet**

L'utilisation d'Internet est soumise à la législation en vigueur. Pour l'accès à Internet depuis le système d'information de l'Énap, les chartes des différents fournisseurs d'accès à Internet ou des solutions hébergées s'appliquent.

L'utilisateur est informé que, si une utilisation résiduelle privée peut être tolérée, les connexions à Internet établies grâce aux ressources du système d'information mises à disposition par l'Énap sont réputées avoir un caractère professionnel. L'Énap, ainsi que les différents fournisseurs d'accès à Internet, peuvent rechercher les connexions à internet établies aux fins de les identifier et de les contrôler conformément aux dispositions prévues par la loi.

Conformément aux dispositions légales, les utilisateurs des services Internet s'engagent à ne pas utiliser les ressources du système d'information pour tenir des propos (oraux ou écrits) à caractère insultants, diffamatoires, racistes, pédophiles ou attentatoires au respect d'autrui, à ne pas porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité notamment par des messages, textes ou images provocants et à ne pas émettre d'opinion personnelle étrangère à son activité professionnelle ou susceptible de porter préjudice à l'administration. Les utilisateurs sont fortement encouragés à respecter les règles de politesse d'usage sur Internet.

Pour assurer la sécurité des équipements connectés et des utilisateurs, il existe un système de pare-feu et de filtrage d'accès internet sans pour autant porter atteinte à la vie privée de qui que ce soit.

L'annuaire des sites Internet proscrit utilisé par l'Énap, est fourni par des universités ou sociétés spécialisées dans la sécurité numérique.

L'accès internet est sécurisé et surveillé par :

- Un dispositif de filtrage des sites non autorisés : pornographie, pédophilie, haine raciale, apologie de tout type de crime et délit, contenu et téléchargement illégaux, etc. ;
- Un système de surveillance qui limite ou interdit de télécharger du contenu ou des logiciels ne respectant pas les besoins et ressources pédagogiques ou administratives.

Le filtrage et la surveillance des connexions est permanent. Les ressources filtrées ne peuvent être débloquent qu'à des fins pédagogiques ou administratives après accord du département informatique et de la direction de l'Énap.

En cas de surconsommation d'internet ou de souci de sécurité, le département informatique peut alerter la direction de l'Énap afin de faire appliquer la présente charte.

L'Énap se réserve tout droit de fermer l'accès à des sites ou à des services internet pour assurer la protection et la disponibilité du réseau internet à ses utilisateurs.

L'Énap se réserve le droit de fermer la connexion internet sans préavis avec l'accord du Directeur de l'Énap ou de son représentant pour assurer la protection de son réseau.

Conformément à la réglementation en vigueur, tout accès sur l'internet est enregistré et journalisé. Ces données sont conservées pendant un an et accessibles aux autorités judiciaires sur réquisition.

4.1.1 Téléchargement ou transfert de fichiers

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

L'Énap se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour les ressources du système d'information (virus susceptibles d'altérer le bon fonctionnement du SI de l'Énap, codes ou logiciels malveillants, programmes espions, etc.).

4.2 Utilisation du réseau privé virtuel Justice (Intranet Justice)

L'utilisation du réseau intranet Justice est conditionnée à la signature et au respect de la charte d'usage des services numériques du ministère de la Justice.

5. Communications électroniques

5.1 Adresses électroniques

L'Énap met à la disposition des utilisateurs deux boîtes à lettres professionnelles nominatives lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de ces adresses nominatives sont ensuite de la responsabilité de l'utilisateur.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement des coordonnées administratives : il ne retire en rien le caractère universitaire de la messagerie.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un *utilisateur* ou un groupe d'*utilisateurs* pour les besoins de l'Énap. Les adresses nominatives ne peuvent pas être partagées entre plusieurs *utilisateurs*.

La gestion des adresses électroniques correspondant à des listes de diffusion, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité de l'Énap : ces listes ne peuvent être utilisées sans autorisation explicite. Leur demande de création à l'initiative d'un utilisateur doit être validée par son responsable avant demande de création auprès du DSI.

L'utilisateur est informé que l'Énap pourra prendre des mesures de type conservatoire sur les comptes de messagerie lorsque la situation le justifie (exemple : blocage de compte en cas de suspicion de compromission, d'usage illicite ou contraire aux dispositions de la présente charte).

5.2 Contenu des messages électroniques

Les règles fondamentales de la correspondance administrative s'appliquent aux courriers électroniques professionnels, s'agissant notamment du choix des destinataires et du respect de la hiérarchie.

L'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges par courrier électronique. Il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'administration. A ce titre, l'utilisateur s'engage à ne pas utiliser les listes de diffusion pour l'envoi de messages à caractère personnel. L'utilisateur doit également veiller au respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique et diffamatoire.

Les courriers électroniques comportant des contenus à caractère illicite sont interdits, quelle qu'en soit la nature. Il s'agit notamment des contenus contraires à la liberté d'expression ou portant atteinte à la vie privée d'autrui au code de déontologie du service public pénitentiaire et plus généralement aux dispositions de l'article 2.4.

L'utilisateur a l'obligation de ne jamais répondre aux pourriels ou relayer les chaînes de messagerie même dans le but d'informer ou alerter d'autres utilisateurs.

L'utilisateur s'engage à ne pas développer ni diffuser de son plein gré, par messagerie, des programmes qui s'auto-dupliquent ou s'attachent à d'autres programmes (virus informatiques, vers, chevaux de Troie).

Afin de ne pas encombrer les ressources du réseau, l'utilisateur s'engage à privilégier systématiquement l'insertion de liens vers un document plutôt que d'attacher le document lui-même en pièce jointe.

Si l'utilisateur reçoit par erreur un message pour lequel il n'aurait pas dû être destinataire, toute utilisation, copie ou diffusion, même partielle de ce message est interdite. Il a l'obligation de le détruire et d'en informer immédiatement son expéditeur.

Par ailleurs, l'utilisation de la messagerie personnelle à des fins professionnelles est fortement déconseillée, du fait de l'exposition de l'organisme à un risque de fuite d'information et ne peut être réalisé qu'en cas de nécessité impérieuse.

En cas de transfert d'information sensibles, l'utilisateur doit se reporter à l'article 4.7.1.3 et .4 de la présente charte.

Tout message est réputé professionnel (en lien avec les activités de l'Énap) sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un répertoire privé de données. En ce sens, il appartient à l'utilisateur de procéder au stockage de ses messages électroniques à caractère privé dans un dossier prévu explicitement à cet effet nommé « PRIVE » ou « PERSONNEL ».

Pour préserver le bon fonctionnement des services, l'Énap se réserve le droit de mettre en place des limitations, dont les termes seront précisés et portés à la connaissance de l'utilisateur par l'Énap.

5.3 Émission et réception de 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, eux-mêmes en petit nombre, afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

Lors d'envois à un nombre important de destinataires, il est recommandé d'utiliser la fonction copie conforme invisible (Cci) du client de messagerie pour inclure la liste des destinataires.

De manière générale, l'utilisateur s'engage à ne jamais utiliser ou fournir son adresse professionnelle ou celle d'un collègue pour poster des messages sur des listes de diffusion externe ou sur Internet.

Il doit veiller plus particulièrement au contenu de son message et à la qualité de son destinataire lorsqu'il émet des données à caractère personnel.

5.4 Émission de messages comportant des données à caractère personnel

L'utilisateur doit veiller plus particulièrement au contenu de son message et à la qualité du destinataire lorsqu'il émet des données à caractère personnel.

En cas d'erreur de destinataire, d'erreur dans le contenu du message ou de la pièce jointe concernant des données à caractère personnel ; l'utilisateur doit avertir sans délai le DPD à dpo.enap@justice.fr pour définir s'il y a lieu d'une violation de données, conformément aux articles 33 et 34 du RGPD.

5.5 Statut et valeur juridique des messages

Les messages électroniques échangés avec les tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1369-1 à 1369-11 du code civil.

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

5.6 Stockage et archivage des messages

Chaque utilisateur doit mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

Pour ce faire il doit stocker ses archives sur un espace du réseau et non en local sur sa propre machine.

5.7 Messagerie instantanée et réseaux sociaux.

L'utilisation des messageries instantanées et des réseaux sociaux pour l'échange d'information professionnelle est strictement prohibée.

Seul le service de la communication de l'Énap est autorisé à en faire usage dans le cadre strict de la promotion et de la communication des activités de l'Énap.

La direction de l'Énap pourra autoriser de manière ponctuelle et encadrée l'utilisation de ces outils.

6. Continuité de service

Afin d'assurer la continuité de service, les personnels de l'Énap doivent privilégier le dépôt de leurs fichiers de travail sur des espaces partagés avec l'ensemble du service ou de l'équipe.

Également, dans la mesure du possible, les personnels de l'Énap doivent favoriser l'usage des alias de messagerie fonctionnels (Exemple : sg-info.enap@justice.fr).

Lors du départ programmé d'un agent, le responsable hiérarchique prévoit le transfert des données professionnelles de l'agent partant (documents et messagerie), en concertation avec celui-ci.

En tout état de cause les données non situées dans le répertoire « PRIVE » ou « PERSONNEL » sont considérées comme des données appartenant à l'Énap qui pourra en disposer.

En cas d'absence, il est recommandé aux personnels de l'Énap de mettre en place un message d'absence associé à leur messagerie. Ce message d'absence pourra préciser une autre personne à contacter durant l'absence. En cas de besoin, pour répondre à la nécessité de service, un message d'absence pourra être mis en place par le DSI, à la demande du responsable hiérarchique du personnel.

Dans le cas où il serait nécessaire d'accéder aux données professionnelles d'un personnel de l'Énap en son absence et afin d'assurer la continuité de service, seul le directeur de l'Énap peut donner son accord, dans le respect du droit à la vie privée et des dispositions de la loi Informatique et Libertés. Le directeur signifiera alors son accord par écrit au responsable du DSI et au responsable du service dont dépend la personne, en précisant les données auxquelles il est nécessaire d'accéder.

L'accès aux données se fera toujours en présence du responsable de service dont dépend la personne concernée.

6.1 Devoir de signalement et d'information

L'utilisateur doit avertir son responsable ou le RSSI de toute anomalie ou dysfonctionnement constaté. Il signale également à son responsable toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

L'utilisateur doit avertir son responsable, le DPD et le RSSI en cas de doute concernant la divulgation possible de données dans les plus brefs délais.

7. Exploitation et contrôle

7.1 Les ressources du système d'information

Les ressources du système d'information de l'Énap font l'objet de contrôles ayant comme unique finalité d'assurer la sécurité et la continuité des ressources et des données de l'Énap. En cas d'événement ou d'anomalie liés à la sécurité ou à la continuité de ses systèmes, l'Énap s'autorise à prendre toutes les mesures nécessaires pour en identifier les causes.

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'Énap se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources du système d'information ;
- que toute action de prise en main à distance (principalement sur les postes de travail) doit obligatoirement être précédée d'un accord de l'utilisateur (sauf cas d'urgence ou mise en péril de la sécurité ou de la continuité de service) ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée et le cas échéant supprimée ;
- que les ressources du système d'information peuvent donner lieu à une surveillance et à un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle des systèmes d'information (administrateurs système) sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

En tout état de cause, les administrateurs systèmes sont soumis au secret professionnel et a un devoir de loyauté, ils ne peuvent communiquer ni utiliser les informations auxquels ils ont accès durant leurs missions

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article 40, alinéa 2 du code de procédure pénale.

A ce titre, l'Énap se réserve le droit de consulter de manière exceptionnelle le contenu des documents, des fichiers ou des messages identifiés « privé » ou « personnel » de l'utilisateur en cas de risque de mise en péril de son activité (par exemple la présence de code malveillant, ou dans le cas d'une enquête judiciaire en cours).

La collecte de données personnelles sera limitée aux informations strictement nécessaires à la sécurité des services et des ressources du systèmes d'information.

Ces données sont conservées pour une durée maximale de 6 mois après collecte.

Les éléments découverts à l'occasion d'une opération de contrôle ou de maintenance sont susceptibles de constituer des moyens de preuves licites contre les agissements d'un utilisateur.

7.2 Autres moyens de télécommunications

L'Énap met à disposition des utilisateurs des moyens téléphoniques fixes ou mobiles.

Ces dispositifs génèrent des données quant à leurs utilisations.

Ces données sont issues des autocommutateurs pour les lignes fixes et des opérateurs pour les lignes mobiles.

Des contrôles administratifs sont effectués régulièrement pour connaître les états de consommations.

Le cadre général de ces contrôles permet d'identifier les lignes non utilisées ou de redéfinir une stratégie d'achat des abonnements.

En cas d'utilisation ou de données non conforme de ces moyens, l'Énap se réserve le droit d'analyser plus finement leurs utilisations et de sanctionner les usages non conformes

8. Traçabilité

L'Énap est dans l'obligation légale de mettre en place un système de journalisation de certains usages des ressources du système d'information, tels que les accès Internet, les accès applicatifs, la messagerie et les données échangées.

Les conditions de collecte et d'utilisation des journaux sont décrites dans le document « Politique de gestion des journaux informatiques à l'Énap », joint à la présente charte.

9. Lois et réglementations applicables

9.1 Propriété intellectuelle

L'Énap rappelle que l'utilisation des ressources du système d'information implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tout tiers titulaire de tels droits.

En conséquence, chaque utilisateur doit :

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

9.2 Réglementation à l'égard de traitement des données à caractère personnel

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée et conformément au règlement européen (UE) 2016/679 relatif à la protection des personnes physiques et du traitement des données à caractère personnel communément appelé Règlement Général sur la Protection des Données (RGPD).

Les données à caractère personnel au sens de l'article 4 du RGPD sont des informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent. Toutes les créations 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 loi « Informatique et Libertés » et le RGPD.

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement le DPD qui prendra les mesures nécessaires au respect des dispositions légales.

Le directeur de l'Énap validera tout traitement avant sa mise en application.

9.3 Traitement de données à caractère personnel non déclaré

Toute mise en application d'un traitement de données à caractère personnel n'ayant pas fait l'objet d'une inscription au registre des traitements et reçu le visa du représentant du responsable de traitement sera considéré comme illégal.

L'Énap et par extension son directeur ne pourra être tenu responsable de ce traitement.

Le propriétaire de ce traitement engagera de facto sa responsabilité civile et pénale en tant que responsable de traitement conformément à la réglementation en vigueur.

9.4 Droits des personnes concernées

Conformément aux dispositions de la réglementation, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des ressources du système d'information.

Ce droit s'exerce auprès du DPD en le saisissant par messagerie à dpo.enap@justice.fr.

Une réponse sous trente (30) jours sera apportée à la personne concernée par retour mail ou par courrier par le DPD.

Le RGPD, en son article 12, dispose que les personnes concernées soient informées de leurs droits de manière concise, transparente, compréhensible et aisément accessible.

Pour ce faire, les droits et devoirs des personnes concernées et de l'Énap sont consultables dans la Politique de protection des données à caractère personnel de l'École Nationale d'Administration Pénitentiaire.

Ces documents sont consultables sur l'Intranet de l'Énap ou auprès du DPD à dpo.enap@justice.fr

Les clauses de cette politique se déclinent suivant l'utilisateur susvisé.

9.5 Politique de Sécurité des Systèmes d'Information de l'Etat

L'utilisateur et l'Énap sont tenus de respecter les dispositions légales et réglementaires suivantes :

- Circulaire PM N°5725, signée le 17 juillet 2014, portant sur la mise en œuvre de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE)

9.6 Protection du secret de la défense nationale et protection des systèmes d'informations sensibles

L'utilisateur et l'Énap sont tenus de respecter l'instruction générale interministérielle n°1300/SGDSN/PSE/PSD du 13 novembre 2020 sur la protection du secret de la défense nationale (IG1300) qui détermine les rôles et responsabilités ainsi que les exigences liées à la gestion du cycle de vie d'une information ou d'un support classifié.

L'utilisateur et l'Énap sont tenus de respecter l'instruction générale interministérielle n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensible

9.7 Protection du potentiel scientifique et technique de la nation

L'utilisateur et l'Énap sont tenus de respecter les dispositions légales et réglementaires suivantes :

- Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation.
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.
- Circulaire interministérielle de la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation du 7 novembre 2012.

9.8 Autres lois et réglementations applicables (liste non exhaustive)

L'utilisateur et l'Énap sont tenus de respecter les dispositions légales et réglementaires suivantes, cette liste se veut non exhaustive :

- La charte d'usage des services numériques du ministère de la Justice ;
- la charte des utilisateurs du Réseau Privé Virtuel Justice ;
- le code de déontologie du service public pénitentiaire ;
- le règlement intérieur de l'Énap ;
- la loi Informatique et libertés du 06 janvier 1978 modifiée ;
- le Règlement Général sur la Protection des Données (UE) 2016/79 (RGPD) ;
- la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ;
- la loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunication ;
- le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques ;
- les articles L.323-1 et suivants du Code Pénal, relatifs aux atteintes aux systèmes de traitement automatisé de données ;
- la loi n°2004-575 du 21 juin 2004 pour la confiance en l'économie numérique ;
- la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique ;
- l'article 9 du code civil relatif au droit à la vie privée ;
- l'article 8 de la convention européenne des droits de l'Homme
- les articles R226-1 et suivants, R623-4 et R625-9 du code pénal relatifs aux atteintes à la vie privée ;
- l'article 227-23 du Code Pénal, relatif à la sanction pénale de la consultation habituelle (sur Internet), de l'enregistrement, de la diffusion et de la détention d'images pédopornographiques ;
- les articles R625-7 et suivants relatifs du Code Pénal relatifs à la sanction pénale de l'incitation à la discrimination, à la haine ou à la violence ;
- les articles R624-3 et suivants du Code Pénal relatif à la sanction pénale de la diffamation ;
- les articles 1369-1 à 1369-11 du Code Civil relatifs aux contrats sous forme électronique ;
- Les chartes d'utilisation d'office 365 Enap, MoodEnap, charte d'utilisation du WIFI à l'Énap
- Les règles d'usage de l'Énap concernant le télétravail

10. Sanctions

L'utilisateur est passible de sanctions dans les cas suivants :

- non-respect des règles précédemment définies dans la présente charte ainsi que des modalités définies dans les guides d'utilisation ou chartes d'utilisation établis par l'Énap ;
- abus dans l'utilisation du système d'information à des fins non professionnels.

Dans ces cas de figure, les sanctions applicables à l'utilisateur sont :

- la suspension, suppression ou limitation des accès et droits d'utilisation du système d'information.
- les poursuites disciplinaires, pénales ou civiles prévues par les textes législatifs et réglementaires en vigueur ;

Par ailleurs, le directeur de l'Énap ou son délégué pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Les agents de l'Énap, élèves disposent de la possibilité d'exercer un recours hiérarchique contre cette décision ou d'exercer les voies de recours dont il dispose devant le juge administratif.

11. Durée de validité et révision de la charte

L'Énap se réserve le droit, à sa seule discrétion et sans information préalable, de modifier, supprimer ou ajouter des clauses à ses chartes, et ce à tout moment. Il est donc conseillé aux utilisateurs de se référer régulièrement après acceptation à la dernière version des dits documents. La présente charte du bon usage des ressources du système d'information et du réseau de l'Énap rentre en vigueur dès son acceptation par l'utilisateur et jusqu'à sa prochaine révision.

12. Entrée en vigueur de la charte

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des ressources du système d'information.

La présente charte a été validée en février 2023 par le comité technique de l'Énap

La présente charte a été validée en septembre 2023 par le Conseil d'Administration de l'Énap.

Elle est applicable à compter de ce jour.

Ce document ainsi que toutes ses annexes seront joints au règlement intérieur de l'Énap.



CHARTE RÉGISSANT L'USAGE DES RESSOURCES

du SYSTÈME D'INFORMATION de l'Énap

Énap - 440, avenue Michel Serres - CS 10028
47916 AGEN cedex 9
+33 (0)5 53 98 98 98
www.énap.justice.fr
Intranet : <http://e-nap.énap.intranet.justice.fr>



LinkedIn

EnapCampus

La page officielle de
l'École nationale
d'administration
pénitentiaire



POLITIQUE DE GESTION DES JOURNAUX INFORMATIQUES

à l'École nationale d'administration pénitentiaire

Février 2023

Table des matières

1. DEFINITIONS ET PREAMBULE.....	2
2. CONTEXTE.....	3
3. PRINCIPES DE BASE	3
3.1 Finalités des traitements	4
3.2 Durée de conservation	4
3.3 Qualités des données collectées	4
3.4 Sécurité et intégrité des données	4
4. LES INTERVENANTS.....	4
4.1 Les utilisateurs.....	4
4.2 La chaîne fonctionnelle SSI.....	4
4.2.1 Les administrateurs systèmes et réseau	5
4.2.2 Les autres acteurs de la chaîne fonctionnelle SSI :	5
5. LES INFORMATIONS ENREGISTREES.....	5
5.1 Informations journalisées par les serveurs (hors messagerie et Web) et postes de travail	5
5.2 Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion...	6
5.3 Serveurs Web	6
5.3.1 Serveurs Web de l'Énap ou applicatif web	6
5.3.2 Serveurs Web hors Énap	6
5.4 La téléphonie sur le réseau internet (ou téléphonie IP)	7
5.5 Les équipements réseau	7
5.6 Les applications spécifiques	7
6. FINALITES DES TRAITEMENTS EFFECTUES ET LEURS DESTINATAIRES..	7
6.1 Résultats statistiques	8
6.2 Résultats d'analyse.....	8
6.3 Détection des usages abusifs.....	8
6.4 Des journaux bruts.....	8
7. DROIT D'ACCES INDIVIDUEL.....	9
8. INFORMATIONS DES UTILISATEURS SUR LA POLITIQUE DE GESTION DES JOURNAUX INFORMATIQUES.....	9
9. ENTREE EN VIGUEUR.....	9

1. Définitions et préambule

Pour une bonne compréhension de la présente politique il est précisé que :

- L'« entité » désigne l'Énap à caractère administratif de l'École Nationale d'Administration Pénitentiaire (Énap)
- L'« utilisateur » désigne toute personne / individu ayant accès ou utilisant les ressources du système d'information de l'Énap, quel que soit son statut, en particulier :
 - Tout agent titulaire ou non-titulaire concourant à l'exécution des missions du service public de l'Énap ou du Ministère de la Justice ;
 - Tout apprenant (stagiaire, élève en formation initiale, continue ou d'adaptation) ;
 - Tout prestataire sous contrat avec l'Énap ;
 - Tout stagiaire utilisant les ressources de l'Énap, y compris les locaux ;
 - Tout lecteur autorisé qui dispose d'un accès aux ressources bibliographiques en ligne ;
 - Toute personne accédant aux ressources en ligne mises à disposition par l'Énap (MOODÉnap, Office 365)
 - Toute personne accédant à un service hébergé par l'Énap, y compris le site internet ;
 - Toute personne accueillie temporairement au sein de l'Énap et ayant de ce fait accès à un poste informatique de l'Énap et/ou au réseau informatique (intervenant pédagogique, invité, etc.).
- Les « ressources du système d'information » désigne l'ensemble des ressources techniques, applicatives, organisationnelles, humaines et documentaires permettant de collecter, stocker, traiter, rechercher et/ou transmettre des données, en particulier :
 - Tout matériel informatique fixe : postes (dont les postes en libre-service), serveurs, téléphones, périphériques (clavier, écran, imprimante, etc.), prises, câbles, ...
 - Tout matériel informatique mobile : ordinateurs, téléphones, etc.
 - Tout logiciel ou service réseau ou informatique : accès réseau, accès Internet, *messagerie* électronique, bureautique, etc.
 - Tout support de données : électronique, papier, etc.
- Le « responsable du traitement » s'entend de, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Au titre de la présente politique, le responsable du traitement est l'École Nationale d'Administration Pénitentiaire (Énap) ;
- Le « délégué à la protection des données » (DPD) et la personne en charge de la protection des données à caractère personnel, il conseille et informe le responsable de traitement. Il est le point de contact avec l'autorité de contrôle (Cnil).
- Les « journaux informatiques » sont les Informations qu'une ressource du système d'information enregistre sur l'activité ou l'identité de ses utilisateurs
- les « personnes concernées » sont les personnes qui peuvent être identifiées, directement ou indirectement et dont leurs données à caractère personnel font l'objet d'une collecte par le responsable du traitement, c'est-à-dire l'ensemble des apprenants de l'Énap ;
- le « destinataire » des données est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Le destinataire des données peut donc être aussi bien le personnel de l'Énap qu'un organisme extérieur (ministère, organismes sociaux, etc.).
- les « données à caractère personnel » : désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Il s'agit des données concernant les apprenants de l'Énap et permettant leur identification ;

- le « traitement de données à caractère personnel » : désigne toute opération ou ensemble d'opérations portant sur des données à caractère personnel, quel que soit le procédé utilisé telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. Il s'agit des traitements (fichiers, bases de données) utilisés par l'Énap pour la gestion administrative et pédagogique de ses apprenants ;
- Les « données sensibles » désigne les données à caractère personnel au sens des articles 9 et 10 du RGPD et de l'article 30 de la LIL concernant le numéro NIR communément appelé numéro de sécurité social. C'est-à-dire, le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. Ainsi que : Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.
L'utilisation, le traitement du NIR ne peut être effectué que pour des finalités dument définies par la réglementation. En aucun cas son utilisation ou conservation ne peut avoir lieu sans consultation formelle du DPD.
Par extension dans la présente, nous incluons les données où le besoin de confidentialité est prégnant (contrat, convention, données ayant trait à la sûreté et la sécurité au renseignement...), l'intégrité (informations de gestion, ...) et la disponibilité nécessitent une protection particulière.

La présente politique de gestion des journaux ne s'applique que pour les traitements dont l'Énap est *responsable de traitement*. En aucun cas cette politique ne s'applique aux autres réseaux comme par exemple le Réseau Privé Virtuel Justice ou aux traitements extérieurs à l'Énap.

Nous invitons les utilisateurs à se rapprocher du responsable de traitement propriétaire de la *ressource informatique* ou du traitement pour connaître leurs droits.

2. Contexte

Le fonctionnement de l'Énap passe par l'utilisation de systèmes d'information et de moyens de communication qui s'appuient sur des réseaux connectés à l'échelle mondiale. Ces réseaux, qui apportent une souplesse inégalée, ont également une vulnérabilité intrinsèque, et leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que dans certaines situations celle de l'Énap qui met ces moyens à leur disposition en tant qu'outils de travail.

L'utilisation des nouvelles technologies de communication pose le problème de la protection d'une part des *données sensibles* gérées par les utilisateurs et d'autre part des systèmes d'information sous la responsabilité de l'Énap. Les mesures mises en œuvre doivent permettre à l'Énap de remplir ses missions tout en satisfaisant aux exigences qui sont imposées par ses engagements vis-à-vis de ses partenaires, des réglementations sur la protection des données sensibles et la protection du patrimoine scientifique, des lois et règlements applicables (voir charte informatique) et en particulier de la réglementation et la loi sur la protection des données à caractère personnel (respect des droits de l'individu) et la sécurité des systèmes d'information.

Une déontologie et un contrôle de l'utilisation sont donc nécessaires, de même qu'une information et une sensibilisation des utilisateurs. L'Énap a mis en place des dispositions et moyens pour assurer la sécurité et le contrôle de l'utilisation des moyens informatiques, et d'autre part a fixé les conditions d'utilisation de ces moyens, afin de garantir les droits individuels de chaque utilisateur.

3. Principes de base

Une maîtrise de la fiabilité et de la sécurité du fonctionnement des systèmes d'information et une garantie de la légalité des transactions opérées. Celles-ci nécessitent un contrôle s'appuyant nécessairement sur l'enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant chaque transaction, appelées journaux informatiques (ou logues).

3.1 Finalités des traitements

Les traitements de ces journaux informatiques ont pour finalités :

- de contrôler le volume d'utilisation de la ressource, de mesurer le trafic et de détecter des anomalies afin de mettre en place une qualité de service et faire évoluer les équipements en fonction des besoins (métrologie) ;
- de vérifier que les règles en matière de sécurité des systèmes d'information (SSI) sont correctement appliquées (tentatives d'intrusion);
- de détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine (activité virale);
- de détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité de l'Énap (pédopornographie);
- de détecter les utilisations des moyens informatiques contraires à la charte informatique de l'Énap.(usurpation d'identité)
- d'être à même de fournir les éléments de preuves nécessaires pour mener les enquêtes en cas d'incident et de répondre à toute réquisition de l'autorité judiciaire présentée dans les formes légales.

Les finalités précitées imposent d'aller au-delà d'un enregistrement et d'une exploitation de données statistiques. Ils impliquent nécessairement l'enregistrement, la conservation temporaire et l'éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettraient de remonter à l'utilisateur.

Ces journaux et leur traitement doivent respecter les droits de chacun et notamment être conformes à la loi du 6 janvier 1978 modifiée dite loi "Informatique et libertés" et du règlement UE 2016/679 dit Règlement général sur la protection des données « RGPD ». Ils doivent avoir satisfait au principe d'information préalable et de transparence.

3.2 Durée de conservation

La durée de conservation des journaux informatiques est de 1 an maximum. L'Énap s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme.

3.3 Qualités des données collectées

Les informations journalisées doivent être factuelles et contextuelles, c'est à dire qu'elles doivent permettre de connaître l'environnement de la collecte, le système hôte, les logiciels mis en œuvre etc. L'heure relevée est une information importante parce qu'elle est souvent le premier élément utilisé pour rapprocher des journaux de différents serveurs. Il est donc indispensable que les machines produisant des logues soient synchronisées sur un serveur de temps.

D'éventuelles interruptions de la journalisation doivent être repérables par les destinataires de ces données.

3.4 Sécurité et intégrité des données

Les journaux contenant des données à caractère personnel doivent être identifiés dans le but de garantir leur suppression au-delà d'une année.

Dans le cas d'une exploitation des journaux informatiques anonymisés, une copie anonymisée des logues est effectuée. L'anonymisation est réalisée dans le respect des règles de l'art, elle est irréversible.

4. *Les intervenants*

4.1 Les utilisateurs

Tous les utilisateurs, tels qu'ils sont définis en introduction de ce document, sont tenus de respecter la charte informatique en vigueur dans l'Énap.

4.2 La chaîne fonctionnelle SSI

En dehors des acteurs de la chaîne fonctionnelle rappelée ci-dessous, personne n'a de droit d'accès aux journaux informatiques comportant des données à caractère personnel, y compris la chaîne hiérarchique. Ils sont tenus au devoir de réserve ou de discrétion professionnelle, voire au secret professionnel.

4.2.1 Les administrateurs systèmes et réseau

Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau et veillent au respect des règles de sécurité des systèmes d'information. À ce titre, ils gèrent les traces dans le respect des obligations générales de leur fonction.

Ils rapportent au *RSSI* et au *DPD* toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau.

Ils acceptent d'exécuter des traitements ou de fournir des informations pouvant inclure des données à caractère personnel uniquement à la demande de la chaîne fonctionnelle de sécurité ou sur instruction écrite du directeur de l'Énap.

4.2.2 Les autres acteurs de la chaîne fonctionnelle SSI :

- les agents du DSI de l'Énap non administrateurs réseau.
- le responsable du Département des systèmes d'information de l'Énap (fonction d'administrateur réseau)
- le Délégué à la protection des données (DPD) (fonction d'administrateur réseau)
- le responsable de la sécurité des systèmes d'information (RSSI) (fonction d'administrateur réseau)
- le responsable de la sécurité des systèmes d'information de l'Administration Pénitentiaire (RSSI DAP),
- le haut fonctionnaire de sécurité de défense (HFSD).

Ils sont également tenus au devoir de discrétion professionnelle, et dans certains cas de secret professionnel en fonction de leur mission.

5. Les informations enregistrées

5.1 Informations journalisées par les serveurs (hors messagerie et Web) et postes de travail

Pour chaque tentative de connexion, d'ouverture de session de travail ou de demande d'augmentation de ses droits, tout ou partie des informations suivantes peuvent être enregistrées automatiquement par les mécanismes de journalisation du service :

- l'identifiant de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- les commandes passées.

Le choix d'une politique de centralisation des journaux informatiques des serveurs (hors messagerie et web) et des postes de travail pourra être mis en place.

5.2 Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion

Les serveurs hébergeant ces services mis en œuvre au sein de l'Énap enregistrent pour chaque message émis ou reçu tout ou partie des informations suivantes :

- l'adresse de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur ;
- l'adresse des destinataires ;
- la date et l'heure de la tentative ;
- les différentes machines traversées par le message ;
- le traitement « accepté ou rejeté » du message ;
- La taille du message ;
- Certaines en-têtes du message, tel que l'identifiant numérique de message ;
- Le résultat du traitement des courriers non sollicités (spam) ;
- Le résultat du traitement antiviral ;
- Les opérations de validation ou de rejet par les modérateurs quand cela s'applique.

Les éléments de contenu des messages ne sont pas journalisés, néanmoins, les applications peuvent inclure des archives qui ne relèvent pas des journaux informatiques (chrono départ et réception).

5.3 Serveurs Web

On distingue les serveurs web exploités au sein de l'Énap de ceux situés en dehors de l'Énap.

5.3.1 Serveurs Web de l'Énap ou applicatif web

Pour chaque connexion, les serveurs Web ou applicatif web, enregistrent tout ou partie des informations suivantes en fonction des exigences de qualité de service et de sécurité de l'application web :

- les noms ou adresses IP source et destination ;
- les différentes données d'authentification dans le cas d'un accès authentifié (intranet par exemple) ;
- l'URL de la page consultée et les informations fournies par le client ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;
- les différents paramètres passés.

5.3.2 Serveurs Web hors Énap

Lorsque les utilisateurs sont des membres de l'Énap, pour chaque accès web via le réseau interne vers des serveurs externes peuvent être enregistrées tout ou partie des informations suivantes :

- les noms ou adresses IP source et destination et les différentes données d'authentification ;
- l'URL de la page consultée ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;

L'article L.34-1 du code des postes et des communications électroniques précise que les opérateurs de communications électroniques sont tenus à une obligation de conservation des données de connexion mais que celles-ci "ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ". Cette interdiction s'applique donc en particulier à l'URL des pages consultées dans le cas où l'Énap offre des accès internet à des personnes extérieures à l'Énap. En effet, il est alors possible d'assimiler le service réseau de l'Énap à celui d'un opérateur de communications électroniques.

5.4 La téléphonie sur le réseau internet (ou téléphonie IP)

L'usage de la téléphonie sur IP peut engendrer des enjeux spécifiques dans le domaine de la sécurité ou dans celui du contrôle du bon fonctionnement des réseaux, mais bien entendu, les principes relatifs à la loi « Informatique et Libertés » s'appliquent à la téléphonie sur IP comme aux autres systèmes de téléphonie.

Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés. Cependant, l'Énap peut éditer des relevés contenant l'intégralité des numéros appelés dans le cas où il demande aux personnels le remboursement du coût des communications personnelles ou dans celui où il a été constaté une utilisation manifestement anormale.

5.5 Les équipements réseau

On appelle « équipements réseau » les routeurs, pare-feu, commutateurs, bornes d'accès, équipement de métrologie et d'administration de réseau, etc. Pour chaque paquet qui traverse l'équipement tout ou partie des informations suivantes peuvent être collectées :

- les noms ou adresses IP source et destination ;
- les numéros de port source et destination ainsi que le protocole ;
- la date et l'heure de la tentative ;
- la façon dont le paquet a été traité par l'équipement ;
- le nombre de paquets et le nombre d'octets transférés ;
- les messages d'alerte.

5.6 Les applications spécifiques

On entend par « applications spécifiques », toute application autre que celles mentionnées ci-dessus qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation.

Parmi ces applications nous pouvons citer les exemples suivants :

- accès aux bases de données ;
- accès à MoodÉnap , Office 365 ;
- service d'authentification (SSO, radius, ...);

Comme dans le cas des serveurs web internes, des journaux génériques sont susceptibles d'être constitués et tout ou partie des informations suivantes peuvent être collectées :

- l'identité de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative ;
- les volumes de données transférées ;
- les commandes passées ;

Le traitement des journaux décrit ici ne couvre pas l'ensemble des données conservées par ces applications qui de par leur nature peuvent historiser certaines transactions. Il est rappelé que si ces données visant à assurer la traçabilité des opérations ont un caractère personnel, elles sont alors soumises aux obligations de la législation portant sur la protection des données à caractère personnel.

6. *Finalités des traitements effectués et leurs destinataires*

Les traitements effectués doivent permettre d'obtenir des journaux qui répondent aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des données à caractère personnel et de la vie privée.

6.1 Résultats statistiques

Ceux-ci sont effectués automatiquement et permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en tant qu'outil de travail. Lors de l'exploitation de ces résultats on s'attachera à distinguer les résultats anonymes de ceux qui peuvent être rapprochés de l'identité d'une personne. Parmi tous ces traitements on trouvera :

- des traitements statistiques en anonyme, en volume transféré et en nombre de connexions ;
- des classements des services les plus utilisés en volume de données et en nombre de connexions ;

Les résultats « anonymes » peuvent être conservés au-delà des délais mentionnés au paragraphe 3.2 et être diffusés sur des sites Internet accessibles à tous. Par contre, les administrateurs systèmes et réseau limitent l'accès aux résultats contenant des données à caractère personnel à eux-mêmes et éventuellement à la chaîne fonctionnelle SSI. La durée de conservation de ces statistiques non anonymisées ne peut excéder celle des journaux utilisés pour produire ces statistiques.

6.2 Résultats d'analyse

Une analyse systématique des traces peut être mise en place, avec l'autorisation du RSSI, afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.

En cas d'incident, des analyses peuvent être faites par les administrateurs systèmes et réseau sur les traces disponibles. Les résultats ne peuvent être transmis qu'à la chaîne fonctionnelle SSI à l'ANSSI ou aux autorités judiciaires pour les incidents de sécurité.

Dans ce cas, l'accès aux journaux est limité aux exploitants des systèmes en charge d'analyser l'incident et au RSSI. L'extraction de l'information et son utilisation sont strictement limitées à l'analyse de l'incident. Si l'incident n'est pas avéré les résultats sont non transmis et immédiatement détruits.

6.3 Détection des usages abusifs

On entend ici par « usages abusifs » les usages du réseau qui sont contraires aux lois ou à la charte informatique. Sont aussi visés les usages qui compromettent les services du réseau de l'Énap tels que :

- consommation excessive de bande passante
- introduction de faille dans la sécurité du réseau
- fichiers volumineux
- envoi massif de messages électroniques
- Etc.

Sont aussi visés les usages qui nuisent au bon fonctionnement de l'Énap, même provenant de l'extérieur tels que

- Appels téléphoniques malveillants
- Messages électroniques malveillants
- Etc.

Les journaux peuvent être exploités pour mettre en évidence ces abus. Par exemple, des classements des machines ayant consommé le plus de réseau en volume transféré et en nombre de connexions permettent souvent de détecter l'utilisation indésirable de protocoles de peer to peer, streaming, ou la présence de serveurs pirates (partage vidéo ou autre).

Quand ils sont mis en œuvre, ces traitements le sont de façon systématique (ils sont appliqués à toutes les machines du réseau de l'Énap ou d'une partie donnée du réseau) et ne ciblent aucune personne ou catégorie de personnes.

6.4 Des journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête. Dès l'apparition d'un incident, les journaux bruts pourront être requis par la chaîne fonctionnelle SSI.

Les administrateurs systèmes et réseau sont chargés de l'application de la requête, et ils sont, pour cette activité, soumis au secret professionnel.

Les journaux bruts sont remis, à sa requête à l'autorité judiciaire afin de lui permettre de poursuivre une enquête.

7. Droit d'accès individuel

Chaque agent peut demander à consulter les traces qui le concernent conformément à l'article 15 du RGPD. Les demandes doivent être faites par écrit auprès du DPD. Conformément à l'article 118 de la loi « informatique et libertés » du 6 janvier 1978 modifiée et à l'article 12 du R.G.P.D., les personnes souhaitant exercer leur droit d'accès doivent justifier de leur identité.

La recherche est faite par l'administrateur, sur demande exclusive du D.P.D.

Les résultats sont transmis personnellement au requérant

8. Informations des utilisateurs sur la politique de gestion des journaux informatiques

L'Énap doit informer ses utilisateurs de la gestion qui est faite des traces qui les concernent.

A cet effet, le présent document sera joint à la charte informatique de l'Énap. Il sera rendu accessible à tout utilisateur par le réseau et notamment :

- via le site web de l'Énap
- via l'intranet de l'Énap
- via OFFICE 365

9. Entrée en vigueur

Le présent document annule et remplace tous les autres documents ou chartes relatifs à la politique de gestion des journaux informatique à l'Énap.

La présente charte a été validée en février 2023 par le comité technique de l'Énap

La présente charte a été validée en septembre 2023 par le Conseil d'Administration de l'Énap.

Elle est applicable à compter de ce jour.

Ce document ainsi que toutes ses annexes seront joints au règlement intérieur de l'Énap.



**POLITIQUE DE GESTION
DES JOURNAUX INFORMATIQUES**
à l'École nationale d'administration
pénitentiaire

Énap - 440, avenue Michel Serres - CS 10028
47916 AGEN cedex 9
+33 (0)5 53 98 98 98
www.énap.justice.fr
Intranet : <http://e-nap.énap.intranet.justice.fr>



LinkedIn

EnapCampus

La page officielle de
l'École nationale
d'administration
pénitentiaire



ORGANISME DE FORMATION
ET DE DÉVELOPPEMENT
DES COMPÉTENCES

440, av. Michel Serres
CS 10028
47916 AGEN cedex 9
+33 (0)6 12 71 88 54

www.enap.justice.fr/organisme-de-formation