

Charte Informatique et Systèmes d'Information EPDSAE

Champs d'application

L'objectif de la présente charte, document d'information et de référence, est de formaliser les règles légales et de sécurité relatives à l'utilisation de tous les outils d'information et de communication au sein de l'EPDSAE.

La mauvaise utilisation de ces outils peut entraîner des risques : risques d'atteinte à la confidentialité, risques d'atteinte à l'intégrité et les sécurités des données (virus, intrusions sur le réseau interne, vols de données, etc.).

Chaque utilisateur doit avoir conscience qu'il a un rôle important dans ce contexte et il s'engage à respecter la présente charte.

La présente charte s'applique à l'ensemble du personnel de l'EPDSAE ayant accès aux outils informatiques.

Gestion des accès

Toute personne définie dans le paragraphe ci-dessus peut disposer d'un droit d'accès au système d'information et aux applications de l'EPDSAE. **Ce droit d'accès est strictement personnel et inaccessible.**

Les droits d'accès sont opérés par la DSI, celle-ci est en charge de :

- **Créer** les accès de l'utilisateur à son arrivée à l'EPDSAE,
- **Modifier** les accès de l'utilisateur si ses missions le nécessitent et sur demande expresse de son supérieur hiérarchique,
- **Suspendre** les accès de l'utilisateur temporairement en cas d'arrêt maladie, de 90 jours ou plus, sur demande expresse de son supérieur hiérarchique et/ou de la Direction des Ressources Humaines,
- **Clôturer** les accès de l'utilisateur lorsque celui-ci quitte définitivement l'EPDSAE ou fait valoir ses droits à congés avant départ en retraite.

Au moment de son départ, l'utilisateur doit restituer les matériels mis à sa disposition et préalablement effacer ses fichiers et données privées.

Accès au poste de travail et aux ressources informatiques

L'utilisation du système d'information nécessite une autorisation d'accès. Celui-ci repose sur un enregistrement de l'utilisateur, lui attribuant un identifiant (login) et un mot de passe, ainsi que les droits d'accès en fonction de ses missions. Cet identifiant et ce mot de passe lui permettent d'accéder à son poste de travail ainsi qu'au réseau interne (*Par exemple, les lecteurs réseaux « Public »*). Il est responsable de l'utilisation de son compte et il lui appartient de ne pas

communiquer son mot de passe à un tiers. Il appartient à l'utilisateur de verrouiller son poste de travail pour toute absence, même de courte durée.

Le mot de passe doit être conforme aux règles mises en place par la DSI. En cas de réception par un administrateur d'un mot de passe temporaire, l'utilisateur doit immédiatement le changer.

Lorsque l'utilisateur est en télétravail ou en déplacement, l'accès au réseau interne doit être effectué au travers d'un VPN sécurisé pour protéger les données échangées et l'utilisateur est le seul à utiliser son poste de travail. En-dehors des locaux de l'EPDSAE, l'utilisateur est responsable en termes de surveillance et d'accès à son poste de travail, le matériel ne doit pas être laissé sans surveillance. L'utilisateur est responsable de l'intégrité de son matériel.

Tout vol ou perte de matériel (PC Portable, Téléphone, etc.) doit être immédiatement signalé à la DSI et tout vol à l'extérieur des locaux de l'EPDSAE doit faire l'objet par l'utilisateur d'une déclaration de vol auprès de la gendarmerie ou de la police.

Toute utilisation contraire aux dispositions de cette charte (Par exemple confier son login et son mot de passe à un collègue) pourra entraîner des sanctions disciplinaires conformément au règlement intérieur.

Accès aux applications

Lorsque les applications le requièrent, leur utilisation nécessite un droit d'accès. Celui-ci repose sur un enregistrement de l'utilisateur, lui attribuant un identifiant (login) et un mot de passe, ainsi que les droits d'accès en fonction de ses missions. Cet identifiant et ce mot de passe lui permettent d'accéder à l'application. Il est responsable de l'utilisation de son compte et il lui appartient de ne pas communiquer son mot de passe à un tiers.

Le mot de passe doit être conforme aux règles mises en place par la DSI et ne doit pas être mémorisé par le navigateur internet. En cas de réception par un administrateur d'un mot de passe temporaire, l'utilisateur doit immédiatement le changer.

Toute utilisation contraire aux dispositions de cette charte (par exemple confier son login et son mot de passe à un collègue) pourra entraîner des sanctions disciplinaires conformément au règlement intérieur.

Certaines applications du SI EPDSAE nécessitent d'être connectées sur le réseau interne car hébergées en interne (Par exemple, *ASTRE RH* et *ASTRE GF*) alors que d'autres ne le nécessitent pas car hébergées en-dehors de l'EPDSAE (Par exemple, *Nemoweb*).

Messagerie électronique

La messagerie électronique est un outil professionnel destiné exclusivement à des usages en lien avec les missions confiées à l'agent. Toute utilisation à des fins personnelles doit rester exceptionnelle et respecter les règles définies par la présente charte.

L'utilisateur s'engage à ne pas envoyer en dehors des services de l'EPDSAE des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel ou autorisé par son supérieur hiérarchique.

Les courriels doivent être rédigés de manière claire, concise et respectueuse, en évitant tout contenu offensant, discriminatoire ou inapproprié. L'objet du message doit refléter précisément son contenu pour faciliter sa gestion par le destinataire. Les destinataires doivent être choisis avec soin afin d'éviter les envois inutiles ou massifs.

En cas d'absence, l'utilisateur doit mettre en place un message d'absence signalant celle-ci.

Toute utilisation abusive ou contraire aux dispositions de cette charte (par exemple, l'envoi de courriels à caractère injurieux ou non professionnel) pourra entraîner des sanctions disciplinaires conformément au règlement intérieur.

Le serveur de messagerie électronique de l'EPDSAE contient les traces des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe.

Accès depuis un matériel personnel

En lien avec les paragraphes 0 et 0, il est précisé que l'EPDSAE autorise l'accès aux ressources suivantes depuis un matériel personnel (smartphone, tablette, ordinateur) par l'usage d'un navigateur internet :

- A la messagerie professionnelle EPDSAE depuis un portail web,
- Aux applications hébergées en-dehors de l'EPDSAE,
- A l'intranet EPDSAE.

Les règles légales et de sécurité relatives à l'utilisation de ces ressources demeurent et l'EPDSAE se réserve le droit de restreindre ces usages.

Usage d'internet

L'accès à Internet fourni par l'EPDSAE est un outil de travail destiné à des usages professionnels. Toute utilisation personnelle doit rester modérée et ne pas nuire à la sécurité des systèmes.

L'accès à des sites à caractère illégal, pornographique, incitant à la haine ou à toute discrimination est strictement interdit. Le téléchargement de logiciels ou fichiers non autorisés est prohibé afin de prévenir les risques de virus, de failles de sécurité et de respecter le droit d'auteur. Les connexions établies via les équipements de l'établissement sont présumées.

Les utilisateurs doivent respecter les mesures de sécurité en place, telles que l'utilisation de mots de passe robustes et la mise à jour régulière des logiciels.

Le pare-feu vérifie tout le trafic internet de l'EPDSAE. En cas d'activité illicite, le pare-feu détient toutes les traces de l'activité qui transite par lui pour la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels).

Il filtre notamment les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

Recommandations sur l'usage des solutions d'Intelligence Artificielle

L'objectif de ce paragraphe est d'informer les agents et de définir les règles d'usage des solutions d'Intelligence Artificielle (IA dans le reste du document) au sein de l'EPDSAE.

La mauvaise utilisation de ces outils peut entraîner des risques : fuites de données sensibles, diffusion de données personnelles, atteinte à la confidentialité des données, etc.

Chaque utilisateur doit avoir conscience qu'il a un rôle important dans ce contexte, il s'engage à respecter la présente charte et à utiliser les solutions d'IA de manière responsable, éthique et sécurisée.

La présente charte s'applique à l'ensemble du personnel de l'EPDSAE ayant accès aux outils informatiques et utilisant une ou plusieurs solutions d'IA.

Les solutions d'Intelligence Artificielle (IA dans la suite du document) sont nombreuses et de nouvelles solutions apparaissent chaque jour, les solutions suivantes sont données à titre d'exemple : Chat GPT, Perplexity, Mistral AI, etc.

L'EPDSAE est conscient que les solutions d'IA sont un levier intéressant et important pour faciliter le quotidien de ses agents depuis la création de contenus à la correction ou reformulation de contenus existants en passant par l'analyse de données chiffrées.

Chaque agent doit être conscient que les solutions d'IA accessibles depuis Internet sont des solutions Cloud avec des conditions générales d'utilisations peu connues du public. Par exemple : ChatGPT stocke les prompts et données de l'utilisateur pour enrichir et améliorer ses modèles au contraire de MistralAI qui ne stocke aucune donnée utilisateur.

Les recommandations de l'EPDSAE sont au nombre de 4 :

1. **Usage responsable** : celles-ci ne doivent pas remplacer la prise de décision humaine ni négliger l'expertise humaine et le raisonnement associé.
2. **Véracité des contenus produits** : les agents doivent être conscients que les contenus produits par les solutions d'IA peuvent être sujettes à des erreurs. L'agent doit faire preuve de discernement face à ces contenus, notamment lorsque ceux-ci sont utilisés pour être partagés en interne ou en externe.
3. **Biais et discrimination** : les solutions d'IA sont entraînées sur des ensemble de données qui contiennent intrinsèquement des biais, des préjugés, les contenus produits par les solutions d'IA peuvent refléter ces biais et/ou préjugés. L'agent doit faire preuve de discernement face à ces contenus, notamment lorsque ceux-ci sont utilisés pour être partagés en interne ou en externe.
4. **Sécurité et confidentialité des données** : l'agent doit respecter les éléments de la présente charte et ne partager aucune donnée personnelle concernant des personnes accompagnées et/ou des agents de l'EPDSAE dans ses interactions avec les solutions d'IA, conformément à l'article 9 de la présente charte. **L'agent doit anonymiser les données soumises aux solutions d'IA.**

Confidentialité des informations

L'utilisateur étant soumis au secret professionnel, à ne pas divulguer d'informations confidentielles vues, entendues, comprises ou déduites dans le cadre de leurs fonctions au sein de l'EPDSAE et à ne les divulguer qu'aux personnes dûment autorisées. Le non-respect du secret professionnel est passible de sanctions disciplinaires conformément au règlement intérieur et constitue un délit pénal passible d'une amende et d'une peine de prison. Les données et informations sont considérées comme privées dès lors qu'elles sont stockées sur le poste de travail dans un dossier nommé « Personnel », « Perso » ou « Privé ».

L'utilisateur est tenu de ne pas utiliser les données et informations à sa disposition à des fins autres que celles prévues dans le cadre de sa mission et de restituer intégralement celles-ci à la cessation de ses fonctions.

Les personnes de la DSI sont amenées à intervenir sur les postes des utilisateurs, les répertoires partagés ou les applications du Système d'information EPDSAE. Ceux-ci s'engagent à ne pas

divulguer d'informations confidentielles vues, entendues, comprises ou déduites dans le cadre de leurs fonctions. Ces agents sont passibles de sanctions disciplinaires conformément au règlement intérieur si un manquement au secret professionnel est constaté.

Lexique

Charte informatique : Document juridique définissant les règles d'utilisation des outils numériques et informatiques mis à disposition par l'EPDSAE, ainsi que les droits et obligations des utilisateurs.

Système d'information : Ensemble des infrastructures matérielles et logicielles et humaines permettant la gestion et le traitement des données au sein de l'EPDSAE.

Autorisation d'accès : Autorisation donnée par le système à un utilisateur dûment authentifié, d'accéder à des données et de procéder à des opérations informatiques en fonction des droits d'accès qui lui ont été préalablement attribués.

VPN : Système de sécurité permettant l'accès au réseau interne de l'EPDSAE depuis l'extérieur, toutes les données entrantes et sortantes du poste de travail sont chiffrées afin de sécuriser la connexion.

Pare-feu : Système de sécurité qui limite le trafic internet entrant et sortant en bloquant les accès non autorisés et/ou ceux présentant des risques.