ÉCOLE DE L'AIR
& DE L'ESPACE
SALON-DE-PROVENCE

ANNEXE 1 du Règlement intérieur général

Charte informatique de l'École de l'air et de l'espace

École de l'air et de l'espace
Base aérienne 701
Chemin St Jean
13300 SALON-DE-PROVENCE
https://www.ecole-air-espace.fr/

Charte informatique de l'École de l'air et de l'espace

Table des matières

Terminologie

Acronyme	Signification
SSI	Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information de l'EAE
PSSI-E	Politique de sécurité des systèmes d'information de l'Etat
RGPD	Règlement général sur la protection des données

ARTICLE 1 : L'objet de la charte

La présente charte définit les règles d'usage et de sécurité de l'EAE que les utilisateurs s'engagent à respecter. Elle précise notamment les droits et les devoirs dans le domaine informatique.

ARTICLE 2 : Définitions

2.1. Ressources informatiques

Le terme « ressources informatiques » désigne l'ensemble du matériel (équipements informatiques, multimédias, téléphoniques, de stockage, d'archivage, de gestion…), les logiciels accessibles en interne ou en externe via le réseau de l'EAE ainsi que les données de l'EAE et les données collectées ou confiées à l'EAE.

Les équipements tiers, notamment personnels, utilisés sur le système d'information de l'EAE dans le respect des consignes de sécurité en vigueur, devient pour le temps de l'usage une ressource informatique de l'EAE et est donc soumis à cette présente charte.

2.2. Services numériques

Les « services numériques » correspondent à l'ensemble des outils et applications (d'échange, de collaboration, …) utilisant des ressources informatiques internes ou externes de l'EAE.

2.3. Utilisateurs

Les personnes utilisant le système d'information de l'EAE, les ressources informatiques s'y rapportant et les services numériques sont appelées « utilisateurs ».

2.4. Administrateurs

Les « administrateurs » sont les utilisateurs chargés officiellement (lettre de mission, poste, contrat de travail, contrat de prestation…) du bon fonctionnement et de la sécurité de ressources informatiques faisant partie du système d'information de l'EAE. Ils sont membres du service en charge des systèmes d'information de l'EAE.

Les « administrateurs systèmes et réseaux » ont la charge de l'installation, du maintien et de la gestion des « équipements techniques ». Ils sont responsables du bon fonctionnement des infrastructures informatiques placés sous leur responsabilité.

Les « administrateurs applicatifs » ont la charge des activités d'exploitation liées aux applications et logiciels de l'EAE ainsi que de la gestion des données. Ils sont responsables du bon fonctionnement des applications et logiciels placés sous leur responsabilité.

ARTICLE 3 : Champs d'application

Les présentes dispositions s'appliquent à l'ensemble des utilisateurs :

- ✓ Au personnel militaire et civil de l'EAE (y compris les stagiaires et apprentis)
- ✓ Au personnel travaillant ou accueillis dans les locaux
- ✓ Aux élèves, étudiants et stagiaires (formation initiale et continue, sous statut civil ou militaire)
- ✓ De manière générale, à l'ensemble des personnes physiques ou morales présentent sur le site de l'EAE ou aillant accès aux systèmes d'information sous la responsabilité de l'EAE (visiteurs, stagiaires, intervenants, personnels d'autres organismes ou administrations, prestataires, invités, membres d'associations, bénévoles…) en présentiel ou en télétravail/à distance.

La charte concerne l'ensemble du système d'information dédié à l'enseignement et à la recherche notamment les ressources informatiques et numériques de l'EAE, y compris celles

auxquelles il est possible d'accéder depuis l'extérieur. Le périmètre INTRADEF est exclu du périmètre de cette charte. La réglementation INTRADEF est déjà encadrée par la politique de sécurité des systèmes d'information des Armées, les instructions ministérielles correspondantes conformément à l'article 23 du RIG.

L'École de l'air et de l'Espace bénéficie d'un accès Internet via le Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche (RENATER).

Tout agissement contraire aux dispositions de la présente charte peut entrainer une suspension temporaire ou définitive des droits d'accès au système d'information et de communication, et est passible, selon la gravité des faits, de sanctions disciplinaires, civiles ou pénales.

Cette charte est annexée au règlement intérieur de l'École de l'air et de l'espace. L'acceptation du règlement intérieur entraine de facto l'acceptation de la présente charte.

ARTICLE 4 : Accès aux ressources informatiques et numériques

4.1. Gestion des accès au système d'information et de communication

L'utilisation des ressources informatiques de l'EAE est soumise à autorisation préalable, concrétisée par l'ouverture d'un compte ou le droit de connecter un équipement informatique ou téléphonique sur le réseau de l'EAE.

Cette autorisation est strictement personnelle et correspond à des privilèges en rapport avec l'activité de l'utilisateur. Elle ne peut donc en aucun cas être cédée à un tiers, même temporairement. Les actions effectuées avec une autorisation d'accès sont imputables à l'utilisateur détenteur de cette autorisation. Un utilisateur ne doit pas utiliser de comptes autres que ceux pour lesquels il a reçu une autorisation. Il doit s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un autre utilisateur. L'utilisateur ne doit pas s'éloigner d'un équipement informatique ou téléphonique mobile sans s'être préalablement déconnecté de sa session ou l'avoir verrouillée.

En cas de ? menace avérée ou de suspicion de menace sur le système d'information de la part d'un utilisateur du SI, après avis du RSSI, l'EAE se réserve le droit de retirer à tout moment l'autorisation de ce dernier, et ce, sans préavis. L'administrateur informera l'utilisateur impacté par tout moyen (mail, téléphone, etc.) permettant une traçabilité.

Enfin, cette autorisation prend fin lors de la cessation de l'activité de l'utilisateur et elle est réexaminée lors de toute modification d'activité (changement de service, changement de catégorie d'utilisateur). Le service des Ressources Humaines notifie à l'administrateur le départ d'un utilisateur dans le cadre du circuit de départ.

Dans ce dernier cas, lors de la fermeture ou de la modification de ses accès accompagnant une mutation ou un départ, l'utilisateur doit laisser ses données professionnelles à disposition de l'EAE et de son ancien service. Par ailleurs, l'utilisateur est responsable avant son départ de la destruction de ses données privées.

Dans le cas particulier des élèves, étudiants et stagiaires, elle prend fin à la diplomation sauf raison exceptionnelle validée par l'École de l'air et de l'espace.

Sauf demande explicite de l'utilisateur, et uniquement dans un but de redirection vers une boite de messagerie électronique externe, l'adresse courriels électronique de l'EAE est supprimée lors de son départ de l'EAE après un délai de 3 mois.

Avant son départ et même en cas de mutation un utilisateur doit restituer au service compétent l'ensemble des équipements qui lui avaient été attribués pour permettre son activité professionnelle.

4.2. Utilisation des ressources

L'utilisation du système d'information et de communication est limitée à des activités légitimes de recherche, d'enseignement, de documentation ou de vie étudiante et militaire, et à toute activité administrative de gestion et de support liée à ces activités.

Ces moyens ne peuvent être utilisés pour une finalité extérieure à l'EAE, sauf autorisation préalable formalisée par une personne ayant autorité pour engager l'EAE.

Tout utilisateur s'engage à utiliser correctement les ressources mises à sa disposition (mémoire à ne pas saturer, espace disque, bande passante des réseaux, imprimantes…). Par exemple, les chaînes de courrier électronique, ou l'envoi d'une pièce jointe lourde à une liste de diffusion sont interdits.

Dans le cadre de l'utilisation d'Internet, seuls les services Internet présentant un lien direct et nécessaire avec l'activité professionnelle ont vocation à être consultés.

L'EAE met en œuvre des actions visant à filtrer l'accès internet pour limiter les sites accessibles ainsi que des mécanismes de collecte des informations de connexion des utilisateurs.

Les restrictions sur les accès internet peuvent être partiellement ou totalement levées, après autorisation du Responsable de la Sécurité des Systèmes d'Information de l'EAE, dans le cas où les besoins métiers des utilisateurs pourraient le justifier.

Une consultation d'Internet pour un motif privé est tolérée (courriels personnels, recherches hors contexte professionnel, etc.) si elle est ponctuelle et brève, si le contenu consulté n'est pas contraire à l'ordre public et enfin si cette consultation n'interfère pas avec les missions confiées à l'utilisateur.

En cas de dysfonctionnement, panne ou perte d'un équipement informatique ou téléphonique ayant pour origine la négligence de l'utilisateur un remboursement à hauteur de la valeur d'usage de l'équipement pourra être exigé.

4.3. Privilèges et droits « administrateurs »

Par dérogation à la PSSI-E, l'utilisateur est autorisé, sur demande dument justifiée et après accord du chef du service en charge des systèmes d'information de l'EAE, à jouir des droits et privilèges administrateurs locaux sur les postes de travail. A ce titre, ils sont soumis aux dispositions de l'article 5.

Le service en charge des systèmes d'information maintient une liste des utilisateurs possédant des privilèges et droits administrateurs.

ARTICLE 5 : Responsabilités des administrateurs du Système d'Information

5.1. Attribution de droits étendus

Les administrateurs sont des utilisateurs jouissant de droits étendus du fait de leur fonction et non de leur position hiérarchique ou à la fiche de poste. Il s'agit des utilisateurs ayant des droits d'administration sur leur poste de travail.

5.2. Devoir de réserve des administrateurs

L'administrateur est soumis dans l'exercice de sa fonction à un devoir de réserve et de confidentialité.

Pour assurer le bon fonctionnement et la sécurité du système d'information et de communication, il peut procéder aux investigations nécessaires (recherche de traces dans les journaux, audit d'un poste de travail, vérification des accès…).

Pour répondre à une réquisition judiciaire, la hiérarchie pourra demander aux administrateurs de communiquer les informations obtenues dans l'exercice de leurs fonctions et entrant dans l'objet de la réquisition.

5.3. Devoir d'information, de conseil et d'alerte

L'administrateur s'engage à informer la Direction Générale de l'EAE des modalités et éventuelles difficultés de mise en œuvre de la politique de sécurité des systèmes d'information et/ou des différentes politiques et procédures.

L'administrateur informe d'urgence son autorité hiérarchique et le RSSI de l'EAE de toute alerte technique et de toute situation d'urgence rencontrées, relatives au système d'information.

L'administrateur s'engage à une obligation générale de conseil, d'information, de recommandation, d'alerte et de mise en garde auprès de la Direction Générale de l'EAE et des utilisateurs.

En outre, l'administrateur assure une veille générale du système d'information et informe le RSSI de l'EAE de tout évènement relatif à la sécurité de l'information. Cette notion concerne le dysfonctionnement qu'il pourrait constater ou de toute information relative à la sécurité. Les incidents de sécurité font l'objet d'une procédure dédiée que l'administrateur doit appliquer.

5.4. Accès aux données personnelles des utilisateurs

L'administrateur peut explorer l'ensemble des fichiers, répertoires, mails/courriels et de manière générale, toutes les données d'un utilisateur à l'exception des éléments indiqués comme « privé » ou « personnel » (l'objet d'un mail courriel est « PRIVE » ou « PERSONNEL », un répertoire est intitulé « Usage privé », « usage personnel » etc.).

L'accès aux données personnelles ne peut se faire qu'en présence de l'utilisateur directement concerné. Seule fait exception à cette règle le cas d'une réquisition de l'autorité judiciaire. Dans ce cas, l'administrateur est autorisé à accéder aux données personnelles d'un utilisateur concerné par cette enquête, sans le consentement de celui-ci.

5.5. Gestion des traces dans le système d'information et de communication

L'administrateur assure l'enregistrement et la gestion des traces et journaux d'événements du système d'information et de communication. Il duplique et assure pendant la durée légale de conservation prévue, la sauvegarde et la conservation des traces et des journaux d'événements.

5.6. Gestion des sauvegardes des données des utilisateurs

L'administrateur peut réaliser la sauvegarde et l'archivage de certains serveurs à risques, y compris ceux hébergeant les données des utilisateurs et le courrier électronique, afin d'assurer la continuité d'activité du système d'information et de communication.

5.7. Gestion des accès d'un équipement informatiques ou téléphoniques

L'administrateur peut interdire tout flux informatique (web, courriel, transfert de fichiers, téléphonie, vidéo, etc.), ainsi que tout équipement informatique ou téléphonique présentant des risques pour la sécurité (virus, rançongiciel, cheval de Troie, etc.), ou en infraction avec la réglementation en vigueur.

Il peut procéder (ainsi que le RSSI de l'EAE) à toute recherche préventive de faille sur les équipements informatiques ou téléphoniques, privés ou non, raccordés au système d'information et de communication. Il peut déconnecter, physiquement ou logiquement, une machine en cas de suspicion.

5.8. Droits de configuration des équipements

En cas d'infection virale ou de panne sur un équipement professionnel fourni par l'EAE, l'administrateur pourra reconfigurer ce matériel dans un état « sortie d'usine » au détriment des données présentes localement.

L'utilisateur reconnait le droit à l'administrateur de réaliser cette tâche, après information de l'utilisateur, même si elle se fait au détriment des données présentes localement sur son matériel.

5.9. Maintenance

Pour effectuer la maintenance corrective, curative ou évolutive, l'EAE se réserve la possibilité de réaliser des interventions (le plus souvent à distance) sur les ressources matérielles et logicielles mises à la disposition des utilisateurs.

Toute situation bloquante pour le système ou générant une difficulté technique, pourra conduire à l'isolement du poste voire à la suppression des éléments en cause et éventuellement, la suspension du compte informatique.

Avant toute prise en main à distance, l'administrateur informe au préalable, et en toute transparence, l'utilisateur concerné et recueille l'accord de celui-ci.

L'administrateur s'interdit d'utiliser ces outils pour exercer un contrôle de l'activité des utilisateurs et, en tout état de cause, les utilisera dans les strictes limites de ses missions. L'administrateur s'engage ainsi à n'accéder qu'aux données nécessaires à l'accomplissement de ses missions et à en assurer la confidentialité.

ARTICLE 6 : Règles générales de sécurité

Chaque utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques de l'EAE. A ce titre, il se doit, à son niveau, de contribuer à la sécurité du système d'information afin de ne pas constituer lui-même un élément de faiblesse pour le système d'information de l'EAE. Notamment :

6.1. Gestion des identifiants informatiques

Tout utilisateur doit choisir des mots de passe sûrs respectant à minima les bonnes pratiques. L'administrateur (ou le RSSI) peut en tester la robustesse.

Ces mots de passe doivent être gardés secrets :

- ✓ Ils ne doivent pas être écrits
- ✓ Ils ne doivent pas être enregistrés dans des systèmes externes à l'EAE (exemple : synchronisation des mots de passe via un navigateur).
- ✓ Dans le cas où un coffre-fort de mot de passe interne est mis en place (Keepass, Bitwarden, etc.), il est nécessaire de l'utiliser

- ✓ En aucun cas être communiqués à des tiers

À la demande des administrateurs (ou du RSSI), ils doivent être changés.

6.2. Mise en œuvre d'outils ayant un impact sur la sécurité du SI

L'utilisation ou le développement de programmes informatiques ou la mise en œuvre de technologies mettant sciemment en cause la sécurité du système d'information et de communication de l'EAE ou des réseaux nationaux ou internationaux (exemples : virus, codes infinis, scanners de vulnérabilités, etc.), sont interdits.

En particulier, l'utilisateur ne peut arguer d'une intention pédagogique ou démonstrative pour être exonéré des sanctions disciplinaires ou des éventuelles poursuites que l'EAE ou l'autorité judiciaire seraient en droit d'engager.

6.3. Devoir de rendre compte

Un utilisateur doit signaler toute violation, tentative de violation ou soupçon de violation du système d'information et de communication dans les délais les plus brefs à l'administrateur et au Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'EAE.

L'utilisateur s'engage à ne pas exploiter les éventuelles failles de sécurité, anomalies de fonctionnement, ou défauts de configuration.

L'administrateur peut prendre la responsabilité de ne pas apporter de correction, si la correction n'est pas disponible ou est considérée comme induisant d'autres problèmes, après avoir informés le RSSI.

6.4. Raccordement des équipements informatiques

L'utilisateur ne doit pas connecter d'équipements informatiques ou téléphoniques sans autorisation du responsable de la sécurité du système d'information et de communication.

La connexion d'un ordinateur ou téléphone mobile privé est permis sur le réseau dédié protégé par portail captif (EA_CAMPUS). Il peut être demandé la création de compte temporaire à destination des visiteurs ou personnels extérieurs sur le réseau EA_GUEST.

Conformément à la présente charte, l'administrateur (ou le RSSI) se réserve le droit de bloquer à tout instant, tout équipement ne respectant pas cette règle.

L'utilisateur a le devoir de protéger les équipements personnels qu'il raccorde aux réseaux dédiés de l'EAE, ou de s'assurer que ceux-ci le sont (antivirus dont les signatures virales sont à jour, mises à jour de sécurité, etc.).

A la demande du RSSI, l'utilisateur doit pouvoir prouver qu'il se conforme à cette obligation.

6.5. Sécurité des données professionnelles

L'utilisateur doit veiller à la sécurité de ses données professionnelles, y compris son courrier électronique, en termes de confidentialité, intégrité et disponibilité. Cela implique de s'assurer qu'une sauvegarde est effectuée à une fréquence adaptée au besoin métier et que leur lieu de stockage est pérenne.

Sauf contrainte particulière (matériel incompatible, législation propre à un pays), le chiffrement est obligatoire dans le cas d'usage d'informatique nomade (ordinateurs portables, téléphone mobiles, clefs USB, disques externes, et tout support de stockage amovible de manière générale). Le service en charge des systèmes d'information met en œuvre ce chiffrement.

L'EAE propose une solution de conteneur sécurisé Zed ![1] permettant l'échange de fichier de manière sécurisée par la création d'une archive chiffrée.

6.6. Utilisation des ressources numériques de l'EAE en externe

En cas de déplacement dans un pays dont la législation interdit le chiffrement de données, ou oblige les utilisateurs à remettre leurs mots de passe ou clefs de chiffrement aux autorités locales, les utilisateurs doivent se conformer aux lois, ne pas importer de matériels chiffrés, et ne pas transporter de données sensibles.

L'usage de services externes (exemples : espace disques, messagerie, bureautique) et les serveurs de données (exemples : Web, FTP, RDP) ne présentant pas de garantie contractuelle de confidentialité, intégrité ou disponibilité est déconseillé. Avant de faire usage de tels services, l'utilisateur doit s'assurer de l'absence de données que leur sensibilité ne rend pas éligibles à ces services (ex : données personnelles, secret industriel, etc.).

Lors d'un départ en mission, notamment à l'étranger, les utilisateurs doivent prendre connaissance des conseils aux voyageurs édictés par l'ANSSI (utiliser des matériels dédiés, sans données sensibles, sans données contraires aux législations locales) :

- ✓ **Avant le voyage :**
  - Relire les règles de l'EAE en matière de SSI
  - Prendre connaissance de la législation locale
  - Utiliser du matériel dédié (ne contenant pas d'information et ne pas transporter de données confidentielles)
  - Sauvegarder ses données et laisser la sauvegarde en lieu sûr (en cas de vol ou de perte de matériel)
  - Utiliser un filtre sur l'écran
- ✓ **Pendant le voyage :**
  - Garder le matériel avec soi
  - Utiliser des mots de passe forts
  - Utiliser le chiffrement
  - Informer l'EAE en cas de perte ou de vol
  - Ne pas utiliser les équipements offerts (clés USB notamment)
  - Ne pas se connecter à des postes qui ne sont pas de confiance
  - Ne pas charger ses équipements sur les bornes libre-service
- ✓ **Après le voyage :**
  - Récupérer les données via une messagerie puis les effacer de l'équipement
  - Changer les mots de passe
  - Faire analyser ses équipements

6.7. Vol d'équipements informatiques ou téléphoniques

En cas de vol, l'utilisateur prévient le plus rapidement son supérieur hiérarchique ainsi que l'administrateur et le RSSI de l'EAE qui prendront les mesures appropriées.

Un dépôt de plainte doit être fait par l'utilisateur qui communiquera la copie du récépissé à l'administrateur et au RSSI.

6.8. Connexion aux réseaux sans fil

L'utilisateur doit être vigilant lors de connexions à des réseaux sans fil peu sécurisés, notamment dans les lieux publics. La sécurité de ces réseaux est faible quand ce ne sont pas des leurres destinés à intercepter les identifiants de l'utilisateur.

[1] Utilisation sécurisée de Zed!

6.9. Règlementation des autorités de tutelle

Lorsqu'il est concerné, l'utilisateur doit respecter les règles définies par son autorité de tutelle tant que celles-ci sont compatibles avec les règles de l'EAE. Dans le cas contraire, les règles de l'EAE priment.

6.10. Boîtes de messagerie électronique de l'École de l'air et de l'espace

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'EAE. L'EAE s'engage à mettre à la disposition de l'utilisateur une boîte aux lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

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

ARTICLE 7 : Respect de la propriété intellectuelle

7.1 Reproduction ou décompilation de logiciels

La reproduction des logiciels commerciaux autre que pour l'établissement d'une copie de sauvegarde est interdite.

La décompilation de logiciels propriétaires est interdite.

7.2 Installation de contenus numériques soumis aux copyrights, droits d'auteur ou DRM

Il est interdit d'installer sur le système d'information et de communication de l'EAE ou tout matériel connecté à ce SI un logiciel, une police de caractères ou tout autre fichier en violation des droits d'auteur, copyrights, DRM et licences associées.

Les licences des logiciels libres doivent naturellement être respectées.

7.3 Logiciels professionnels installés sur un équipement privé

Les logiciels professionnels mis à disposition par l'EAE sur des équipements informatiques ou téléphoniques personnels doivent être supprimés lors du départ de l'EAE.

7.4 Archivage des ressources documentaires

L'usage des ressources documentaires doit être conforme à la politique de gestion documentaire.

Le téléchargement massif et systématique de ressources documentaires par l'intermédiaire d'un robot ou de tout autre logiciel est interdit.

ARTICLE 8 : Respect de la confidentialité des informations

8.1 Droits d'accès aux informations

Tout utilisateur est responsable, pour ses fichiers et répertoires, des droits de lecture et de modification qu'il donne aux autres utilisateurs. Il est cependant interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas correctement protégées. En conséquence, l'utilisateur ne doit pas tenter de lire, copier, divulguer, modifier les fichiers d'un autre utilisateur sans y avoir été explicitement autorisés.

8.2 Hébergement des informations

L'utilisateur doit utiliser les serveurs de partage de fichiers ou de gestion documentaire de l'EAE et de ses partenaires, ainsi que ceux d'un hébergeur validé par le RSSI.

L'usage d'hébergements distants non maitrisés (exemples : non-respect de la protection des données personnelles, absence de contrat de service avec l'EAE, soumission à des lois extraterritoriales, données à usage restreint) est interdit.

8.3 Interception des communications entre tiers

L'utilisateur ne doit pas tenter d'intercepter des communications entre tiers.

8.4 Respect des engagements de confidentialité avec un tiers

L'utilisateur est tenu de prendre les mesures de protection des données garantissant le respect des engagements de confidentialité pris par l'EAE vis-à-vis de ses partenaires.

8.5 Traitement des données nominatives

L'utilisateur est informé de l'obligation de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément au Règlement général sur la protection des données (RGPD – 2016/679) et à la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Le délégué à la protection des données doit être informé de tout projet de traitement de données nominatives sur le système d'information et de communication de l'EAE, afin d'accompagner le responsable du traitement dans la mise en conformité avec le RGPD et notamment dans la mise à jour du registre des traitements de l'EAE.

Les droits d'accès, de rectification, de suppression, de limitation et de portabilité sont exercés auprès du délégué à la protection des données à cette adresse :
eae-referent-dpd@ecole-air.fr
Pour tous renseignements sur la protection des données personnelles, il est possible de contacter le délégué à la protection des données à cette adresse :
eae-referent-dpd@ecole-air.fr

8.6 Continuité de service

En cas d'absence d'un utilisateur, toute mesure indispensable à la continuité du service peut être mise en œuvre qui ne contredise pas les règles décrites dans la présente charte et dans la PSSI-E. Par exemples, le transfert de dossiers, droits d'accès temporaires ou permanents à des personnes ayant le besoin d'en connaître, et comportant les éventuelles habilitations requises).

8.7 Confidentialité des données

L'utilisateur doit être extrêmement vigilant vis-à-vis des données considérées comme confidentielles (données à caractère personnel et informations techniques).

En particulier, il ne doit pas transporter ou déposer sans protection (telle qu'un chiffrement) des données sensibles sur des supports ou services non fiabilisés. L'accès à des données sensibles est interdit depuis des postes ou des réseaux non sûrs.

Le partage de données depuis un poste de travail est interdit (l'utilisateur doit partager ses données via un serveur de fichiers ou un serveur de gestion documentaire autorisés par le RSSI, ou encore la messagerie ou les services de collaboration de l'EAE).

Lors de consultations d'informations sensibles, l'utilisateur doit être vigilant quant aux traces laissées : historique de navigateurs, mots de passe, caches, cookies, etc.

ARTICLE 9 : Relations avec les sites distants et les autres sites informatiques

9.1 Connexion à un site distant

Il est interdit de se connecter ou d'essayer de se connecter à un site distant sans y être dûment autorisé. Tout VPN, mécanisme de contournement de type serveur mandataire "proxy" ou chiffrement réseau mis en œuvre dans un but illégitime ou a fortiori illégal sont interdits.

9.2 Fonctionnement intègre du système d'information

Il est interdit de se livrer depuis des ressources informatiques appartenant à l'EAE ou étant connecté aux réseaux informatiques de l'EAE à des actes mettant sciemment en péril la sécurité ou le fonctionnement du système d'information, local ou distant, et des réseaux de télécommunications ou de nuire à l'image de l'EAE.

9.3 Partage d'information avec un site distant

L'utilisateur doit être vigilant lors de toute saisie d'informations personnelles sur Internet, notamment avec la multiplication des courriers d'hameçonnage (phishing).

L'EAE ne pourra être tenue responsable des dommages subis lors de telles divulgations d'informations.

L'administrateur (ou le RSSI) se réserve le droit de bloquer les accès d'un utilisateur victime d'hameçonnage à des fins de protection du système d'information et de communication et d'audit, et ce pour toute la durée qu'il estime nécessaire.

Le RSSI peut organiser des simulations d'attaque de type hameçonnage sur tout ou partie des utilisateurs dans un but uniquement pédagogique et de sensibilisation. Les résultats de cette simulation sont confidentiels.

ARTICLE 10 : Échanges électroniques

10.1 Devoir de réserve

Dans ses échanges, nul ne peut s'exprimer au nom de l'EAE ou engager l'EAE sans y avoir été dûment autorisé, ou sans que les fonctions qu'il exerce le prévoient.

10.2 Règles de bonne conduite

Chacun doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques (mails, chats, réseaux sociaux, etc.). De plus, l'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

10.3 Responsabilité de l'utilisateur relative au contenu des échanges

Compte tenu de la valeur juridique d'un courriel, chacun doit être vigilant sur leur contenu et s'assurer de leur conservation (un an minimum). Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1174 à 1177 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.

10.4 Intégrité des échanges électroniques

Il est rappelé qu'aucune garantie de bonne transmission et de délai d'acheminement ne peut être apportée aux courriels qui sont émis ou réexpédiés hors de l'EAE, du fait même du fonctionnement d'Internet.

ARTICLE 11 : Évolution de la charte

Cette charte est consultable sur l'espace documentaire de l'EAE, et elle est susceptible de modifications en fonction des évolutions techniques et réglementaires, des usages et de l'organisation de l'EAE. Seule la dernière version française fait foi.

ARTICLE 12 : Sanctions applicables

Tout utilisateur n'ayant pas respecté les dispositions de la présente charte est passible de poursuites internes à l'Administration, civiles ou pénales.