Charte du numérique responsable de l'ICHEC

1. Objet de la charte

La présente Charte du numérique responsable (ci-après la charte) définit les règles d'utilisation des ressources numériques mises à disposition par l'ICHEC Brussels Management School. Elle vise à garantir un environnement numérique :

- sécurisé ;
- respectueux des personnes ;
- conforme aux obligations légales et réglementaires ;
- aligné avec les missions d'enseignement, de recherche et d'administration de l'Institution ;
- attentif aux impacts environnementaux, sociaux et éthiques du numérique.

La charte complète d'autres dispositions et règlements en vigueur au sein de l'institution (règlement des études, règlement de travail, contrat de travail, politique de vie privée, contrat de location…) et en précise certains aspects.

2. Champ d'application

La charte s'applique à l'ensemble des utilisateurs des systèmes d'information de l'ICHEC, à savoir :

- les étudiants ;
- les membres du personnel académique, scientifique, administratif et technique ;
- les intervenants externes et les visiteurs disposant d'un accès aux réseaux ou services numériques de l'Institution.

Elle couvre l'utilisation :

- du matériel informatique (postes fixes, ordinateurs portables, équipements partagés, matériel prêté) ;
- des réseaux filaires et WiFi ;
- des services numériques (messagerie, plateformes d'apprentissage, outils collaboratifs, ressources cloud, systèmes administratifs) ;
- des outils d'intelligence artificielle mis à disposition par l'Institution (Cfr Charte IA).

Toute utilisation des ressources de l'ICHEC implique l'adhésion à la présente charte. Celle-ci s'applique tant au département ICHEC de la Haute Ecole ICHEC – ECAM – ISFSC qu'à l'asbl ICHEC.

3. Principes généraux d'utilisation des ressources numériques

L'utilisation des moyens informatiques de l'ICHEC a pour objet exclusif les activités d'enseignement, de recherche ou d'administration.

Les utilisateurs s'engagent à adopter un comportement responsable et conforme aux législations en vigueur, notamment en matière de protection des données, de respect de la vie privée, de propriété intellectuelle et de cybersécurité.

Il est strictement interdit de :

- masquer son identité ou usurper l'identité d'un tiers ;
- tenter d'accéder à des données ou ressources sans autorisation ;
- consulter, diffuser ou produire des contenus à caractère illicite, violent, discriminatoire, haineux ou pornographique ;
- perturber volontairement le fonctionnement des systèmes ;
- porter atteinte à l'intégrité, à la sensibilité ou à la réputation d'autrui ;
- diffuser des informations confidentielles ;
- diffuser des données personnelles, et notamment des photos ou vidéos sans autorisation des personnes concernées ;
- créer ou diffuser des images textes ou vidéos créées par une IA sans le signaler ;
- créer ou diffuser des fake news sans signaler leur caractère inexact ;
- utiliser les outils informatiques de l'ICHEC à des fins politiques, commerciales, religieuses ou promotionnelles non liées à ses missions.

L'ICHEC rappelle également que le plagiat, sous toute forme, y compris via des outils numériques ou d'intelligence artificielle, constitue une fraude académique (cf. règlement des études).

4. Responsabilité environnementale et sobriété numérique

L'ICHEC encourage une utilisation du numérique consciente de ses impacts environnementaux.

Les utilisateurs sont invités à adopter des pratiques visant à limiter l'empreinte écologique des équipements et des usages numériques.

À ce titre, ils s'engagent à :

- privilégier l'usage des équipements existants et éviter les renouvellements non nécessaires ;
- prendre soin du matériel afin d'en prolonger la durée de vie (protection, entretien, usage adapté) ;
- signaler les équipements défectueux en vue de leur réparation plutôt que leur remplacement systématique ;
- limiter la consommation énergétique liée aux usages numériques (éteindre les équipements non utilisés, paramétrer les modes d'économie d'énergie…) ;
- éviter le stockage et le partage de données non nécessaires (tri régulier des fichiers, suppression des doublons, limitation des pièces jointes volumineuses, usage raisonné du cloud) ;
- privilégier des modes de communication et de travail numériques moins consommateurs de ressources lorsque cela est possible (par exemple, limiter l'usage de la vidéo en continu lorsque cela n'est pas nécessaire) ;
- veiller à un usage raisonné des réseaux (Wi-Fi, données mobiles) en fonction des besoins ;
- respecter les procédures mises en place par l'Institution en matière de gestion de fin de vie des équipements (collecte, réemploi, recyclage).

5. Responsabilité sociale, inclusion et éthique numérique

L'utilisation des outils numériques au sein de l'ICHEC s'inscrit dans le respect des valeurs de l'Institution, notamment en matière d'inclusion, de respect des personnes et d'éthique.

Les utilisateurs s'engagent à :

- adopter un comportement respectueux dans leurs interactions numériques (messagerie, plateformes collaboratives, forums), conforme aux principes de bienveillance et de non-discrimination ;
- ne pas contribuer à des formes de cyberharcèlement, de pression numérique ou de comportements inappropriés en ligne ;
- veiller à un usage mesuré des outils de communication afin de limiter la surcharge informationnelle (usage raisonné du nombre des destinataires, limitation des messages non essentiels, attention portée aux notifications) ;
- respecter le droit à la déconnexion des autres utilisateurs, en évitant notamment les sollicitations en dehors des horaires appropriés, sauf urgence justifiée ;
- porter une attention particulière à l'accessibilité des contenus produits (documents lisibles, formats adaptés, structuration claire, compatibilité avec les outils d'assistance) afin de garantir l'inclusion de tous les utilisateurs ;
- être attentif aux enjeux d'inclusion numérique, notamment en veillant à ne pas exclure des utilisateurs en raison de leurs compétences ou de leur accès aux outils ;
- faire preuve de discernement dans la production et la diffusion de contenus numériques, notamment en vérifiant la fiabilité des informations partagées et en évitant toute forme de désinformation.

6. Règles en matière de cybersécurité

6.1. Accès, authentification et confidentialité

Règles de sécurité critiques :

- Identifiants et mots de passe :
  - **Les codes d'accès sont strictement personnels et confidentiels** : ils permettent d'authentifier l'utilisateur sur les systèmes informatiques de l'ICHEC, y compris dans l'accomplissement de démarches administratives digitalisées. Le partage d'identifiants et mots de passe est formellement interdit.
  - Lors de son inscription ou de son entrée en fonction, l'utilisateur reçoit un mot de passe qu'il est tenu d'utiliser pour tout accès aux systèmes et plateformes informatiques de l'ICHEC. **Ce mot de passe ne doit jamais être communiqué à qui que ce soit, ni être réutilisé pour des comptes personnels extérieurs.** Si l'utilisateur suspecte que son mot de passe a été compromis, il doit immédiatement le modifier et choisir un mot de passe totalement nouveau de minimum 10 caractères, complexe et unique.
- **MFA** (Multi-Factor Authentication) : L'utilisateur s'engage à activer et utiliser la double authentification sur les services le requérant, sans chercher à la contourner, en **utilisant une application d'authentification** (telle que Microsoft Authentificator).
- **Verrouillage de session et déconnexion** : L'utilisateur doit verrouiller sa session (Windows+L) dès qu'il quitte son poste, même pour une courte durée. Il doit veiller également à **se déconnecter** des applications institutionnelles à l'issue de chaque session, en particulier sur les postes partagés (salles informatiques, bibliothèque).

6.2. Protection des équipements

6.2.1. Équipements fournis par l'ICHEC

Les équipements mis à disposition par l'institution (ordinateurs portables, tablettes, téléphones professionnels) sont destinés à un usage professionnel ou académique. Tout utilisateur est tenu de :

- **Maintenir le système d'exploitation et les applications à jour**, en acceptant sans délai les mises à jour proposées par le Centre informatique (CTI) ou les systèmes de gestion centralisée ;
- Ne pas désactiver les **logiciels antivirus et pare-feu** installés par le Centre informatique ;

- Ne pas modifier la **configuration de sécurité** des équipements (désactivation du chiffrement, modification des paramètres réseau, obtention de droits administrateurs non autorisés, etc.) ;
- Prendre soin du matériel ;
- Respecter les procédures d'utilisation (convention de mise à disposition, règles d'utilisation affichées dans les salles…) ;
- Signaler immédiatement au Centre informatique toute panne, anomalie ou dommage constaté ;
- Signaler immédiatement au Centre informatique toute **perte ou vol** d'un équipement institutionnel afin que les accès correspondants puissent être révoqués (voir points de contact ci-dessous) et qu'en cas de violation de données, les déclarations nécessaires puissent être réalisées.

Si l'utilisateur souhaite installer un logiciel, il doit d'abord s'assurer qu'il provienne **d'un éditeur et d'une source de confiance**. Il doit également s'assurer que ce logiciel est distribué sous une **licence autorisée** pour une installation sur un PC de l'ICHEC. En cas de doute sur ces points, il s'adressera au Centre informatique. L'utilisateur ne devra en aucun cas :

- Faire une copie illicite d'un logiciel ;
- Contourner les restrictions d'utilisation d'un logiciel ;
- Installer des logiciels à caractère ludique.

6.2.2. Équipements personnels (BYOD – Bring Your Own Device)

L'utilisation d'équipements personnels pour accéder aux ressources de l'ICHEC est possible sous réserve du respect des conditions suivantes :

- L'équipement doit disposer d'un **système d'exploitation à jour** et supporté par son éditeur ;
- Le Centre informatique se réserve le droit de **refuser l'accès** à ses réseaux à tout équipement non mis à jour et/ou présentant un risque de sécurité identifié ;
- L'accès à certaines ressources institutionnelles sensibles (applications de gestion administrative, comptable, technique…) depuis un équipement personnel n'est pas autorisé.

6.2.3. Supports amovibles

L'utilisation de supports amovibles (clés USB, disques durs externes) représente un vecteur de risque important. En conséquence :

- L'utilisation de supports amovibles personnels sur les équipements institutionnels est déconseillée et soumise à la prudence de l'utilisateur ;
- Tout support amovible trouvé dans les locaux de l'ICHEC ou dont la provenance est inconnue ne doit **jamais être connecté** à un équipement institutionnel sans validation préalable du Centre informatique ;
- Les données sensibles stockées sur un support amovible doivent être **chiffrées**.

6.3. Utilisation du réseau et des connexions Internet

6.3.1. Réseau Wi-Fi

L'ICHEC met à disposition plusieurs réseaux sans fil distincts selon les profils d'utilisateurs. Chaque utilisateur est tenu de :

- Se connecter **uniquement au réseau Wi-Fi qui lui est attribué** en fonction de son profil (réseau staff et étudiants « ICHEC », réseau invité « ICHEC-GUEST », réseau de mobilité interuniversitaire « eduroam ») ;
- Ne pas tenter d'**accéder aux réseaux réservés** à d'autres catégories d'utilisateurs ;
- Ne pas créer de **point d'accès Wi-Fi non autorisé** (partage de connexion) susceptible de contourner les politiques de sécurité du réseau institutionnel.

6.3.2. Utilisation d'Internet à l'ICHEC

L'utilisateur s'engage à ne pas :

- Utiliser des **outils d'anonymisation** (proxies non autorisés, réseaux Tor) pour contourner les politiques de filtrage de l'institution ;
- Accéder à des **sites illégaux ou malveillants**, notamment des sites de téléchargement illicite, de jeux d'argent non autorisés ou hébergeant des contenus contrefaits ;
- Effectuer toute **action à caractère malveillant ;**
- Effectuer des **transactions financières personnelles sensibles** depuis les équipements ou réseaux partagés de l'institution.

6.3.3. Réseaux Wi-Fi publics et accès distant

Lorsqu'un utilisateur accède aux ressources de l'ICHEC depuis l'extérieur de l'établissement :

- Il est **formellement déconseillé** d'accéder à des ressources institutionnelles depuis un réseau Wi-Fi public non sécurisé (aéroport, gare, café, hôtel, autres lieux publics…) ;

- Tout incident de sécurité survenu dans ce contexte doit être **signalé immédiatement** au Centre informatique afin de prendre les mesures appropriées, notamment si des données personnelles sont concernées.

6.4. Gestion des données et confidentialité

6.4.1. Classification et protection des données

Les utilisateurs amenés à manipuler des données dans le cadre de leurs activités à l'ICHEC doivent être attentifs à la sensibilité des informations traitées. On distingue notamment :

- Les **données publiques** : librement accessibles et diffusables ;
- Les **données internes** : réservées à l'usage interne de l'institution ;
- Les **données confidentielles** : incluant les données personnelles au sens du RGPD, les données financières, les données relatives aux délibérations, etc. Ces données ne peuvent être partagées qu'avec les personnes habilitées et selon les canaux sécurisés prévus à cet effet.

6.4.2. Conformité au RGPD

Conformément au Règlement Général sur la Protection des Données (UE) 2016/679, tout utilisateur amené à traiter des données à caractère personnel dans le cadre de ses activités à l'ICHEC est tenu de :

- Ne collecter et traiter que les données **strictement nécessaires** à la finalité poursuivie (principe de minimisation) ;
- Respecter les finalités, les durées de conservation et les autres principes de traitement de données tels que définis par les **politiques de gestion des données à caractère personnel** de l'ICHEC ;
- Ne pas **transférer de données personnelles** de tiers vers des services cloud et des services d'intelligence artificielle non approuvés par l'institution ;
- De manière générale, **s'abstenir d'utiliser des services tiers** (matériel ou logiciel) non approuvés par le Centre informatique pour traiter ou stocker des données personnelles (« shadow IT ») ;
- Signaler sans délai au **Délégué à la Protection des Données (DPO)** de l'ICHEC tout incident susceptible de constituer une **violation de données personnelles** (accès non autorisé, perte de données, envoi à un mauvais destinataire, etc.) – voir point de contact ci-dessous.

Tout accès à des systèmes ou données dans un cadre d'enseignement, de recherche ou d'administration doit se faire dans le **strict respect des droits qui ont été accordés**, sans tentative d'élargissement non autorisé des privilèges.

6.4.3. Stockage et sauvegarde des données

Afin de garantir l'intégrité et la disponibilité des données institutionnelles :

- Les données professionnelles ou académiques doivent être **stockées prioritairement sur les espaces de stockage institutionnels** (serveurs, espaces cloud approuvés par l'ICHEC, tels que SharePoint), et non exclusivement sur le disque local d'un équipement ;
- Il est **interdit** de stocker des données sensibles de l'institution sur des services de cloud public personnels (Google Drive personnel, Dropbox personnel, etc.) sans autorisation du Centre informatique ;
- Chaque utilisateur est responsable de la **sauvegarde régulière** des données dont il est le seul dépositaire et de la destruction de celle-ci lorsqu'elles sont devenues inutiles.

6.4.4. Chiffrement

Pour les données particulièrement sensibles (données personnelles, données confidentielles) :

- L'utilisation d'outils de **chiffrement approuvés** par le Centre informatique est recommandée, et peut être rendue obligatoire pour certaines catégories de données ou d'équipements (notamment les ordinateurs portables) ;
- Les utilisateurs ne doivent pas tenter de **contourner ou désactiver** les mécanismes de chiffrement mis en place par l'institution.

6.4.5. Fichiers de traces (logs)

Les utilisateurs sont informés que les différents services utilisés génèrent, à l'occasion de leur emploi, « des fichiers de traces » (logs). Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations concernant, par exemple, la messagerie (expéditeur, destinataire(s), date), mais aussi les heures de connexion aux applications de gestion, au service de connexion à distance, le numéro de la machine depuis laquelle les services sont utilisés, etc. Ce type de traces existe pour l'ensemble des services internet. Ces fichiers ne sont utilisés que pour un usage soit technique, soit imposé par la loi.

6.5. Vigilance face aux cybermenaces

6.5.1. Hameçonnage (phishing) et ingénierie sociale

Le phishing constitue aujourd'hui le principal vecteur d'attaque informatique. Tout utilisateur est tenu de :

- Se montrer **systématiquement vigilant** face aux courriels, messages ou appels téléphoniques non sollicités demandant des informations confidentielles, des identifiants, ou incitant à cliquer sur un lien ou à ouvrir une pièce jointe ;
- **Vérifier l'identité de l'expéditeur** avant tout clic sur un lien ou ouverture de pièce jointe, notamment en cas de message urgent ou inhabituel, y compris si l'expéditeur apparent est un collègue ou un membre de la direction ;
- **Ne jamais communiquer ses identifiants** à la suite d'une demande reçue par courriel, même si celle-ci semble provenir du Centre informatique ;
- **Signaler immédiatement** au Centre informatique tout courriel suspect, sans y donner suite, en utilisant le canal de signalement prévu à cet effet ;
- **Signaler immédiatement toute réponse à une tentative de phishing afin que le CTI puisse prendre les mesures appropriées.**
- En cas de **doute sur une communication**, contacter directement l'expéditeur supposé par un canal distinct (téléphone, contact en personne) pour en vérifier l'authenticité.

6.5.2. Logiciels malveillants (malwares)

Pour réduire le risque d'infection par des logiciels malveillants (virus, ransomware, spyware, etc.) :

- L'utilisateur ne doit **télécharger des logiciels ou des fichiers** que depuis des sources officielles ;
- Il ne doit jamais **se connecter à des sticks USB ou des disques durs externes** qui ne lui appartiennent pas ou qui ne soient pas proposés par le CTI ;
- Il ne doit pas **désactiver ou contourner** les protections antivirales et les filtres de sécurité en place ;
- En cas de **comportement anormal** d'un équipement (lenteur inexpliquée, messages d'erreur inhabituels, activité réseau suspecte), l'utilisateur doit **cesser toute activité sensible** et contacter immédiatement le Centre informatique ;
- En cas d'infection avérée ou suspectée, l'équipement concerné doit être **isolé du réseau** (déconnexion du Wi-Fi et du câble réseau) dans les meilleurs délais.

6.5.3. Usurpation d'identité numérique

Il est rappelé qu'il est strictement interdit de :

- **Se faire passer pour une autre personne** (collègue, enseignant, membre de la direction, technicien informatique) dans le cadre de communications électroniques ;
- **Utiliser le compte d'un autre utilisateur**, même avec son accord apparent ;
- Procéder à toute tentative de **reconnaissance ou d'interception de trafic réseau** (sniffing).

6.6. Messagerie électronique et outils collaboratifs

6.6.1. Messagerie institutionnelle

L'adresse de messagerie électronique institutionnelle attribuée par l'ICHEC est un outil de communication officiel. Son utilisation implique les responsabilités suivantes :

- **Utiliser la messagerie institutionnelle** pour toute communication officielle avec l'ICHEC, les enseignants ou les collègues, et non une adresse personnelle ;
- Ne pas utiliser la messagerie institutionnelle pour **diffuser des messages en masse** (chaînes de messages, publicités, communications à caractère politique ou commercial) ;
- Être **attentif avant de répondre ou de transférer** un message contenant des informations confidentielles ou sensibles, en vérifiant l'identité et la légitimité du ou des destinataires ;
- En cas de messages destinés à un groupe de personnes (au-delà de 4), il est recommandé de **mettre les adresses emails en BCC**.

6.6.2. Outils collaboratifs et plateformes numériques

L'ICHEC met à disposition ou approuve l'utilisation de certains outils collaboratifs (plateformes de visioconférence, espaces de travail partagés, outils de messagerie instantanée… ex : Teams, SharePoint…). En dehors de ces outils approuvés :

- L'utilisation d'outils collaboratifs **tiers non approuvés** pour échanger des données institutionnelles sensibles n'est pas autorisée ;
- Lors de sessions de **visioconférence**, l'utilisateur veille à ne pas partager d'informations confidentielles dans un environnement où des tiers non autorisés pourraient y accéder (espace public, session ouverte à des participants non identifiés).

NB : les réseaux sociaux ne sont pas reconnus par l'institution comme outils officiels de communication et de collaboration interne. Dans le cadre institutionnel, ils ne sont utilisés qu'à des fins promotionnelles.

6.6.3. Intelligence artificielle générative

L'utilisation croissante d'outils d'intelligence artificielle générative (tels que ChatGPT, Copilot, Gemini, etc.) nécessite une vigilance particulière :

- Les utilisateurs sont informés que les contenus soumis à certains de ces services peuvent être **traités et potentiellement conservés** par des tiers hors du contrôle de l'ICHEC, notamment à des fins d'entraînement des modèles de langage ;
- Il est **interdit d'introduire dans ces outils** des données confidentielles de l'institution, des données personnelles ou tout autre contenu couvert par le secret professionnel, sauf dans le cas de services d'intelligence artificielle reconnus par l'institution et dans les limites fixées par celle-ci ;
- En pratique, le Centre informatique communiquera, le cas échéant, une liste d'outils approuvés et les conditions de leur utilisation dans le cadre institutionnel.

L'usage des outils d'intelligence artificielle à l'ICHEC est balisé par une « Charte IA » qui précise et complète les présentes dispositions.

7. Responsabilités des administrateurs système et réseau

Les administrateurs système et réseau sont chargés :

- d'assurer la continuité, la sécurité et la qualité des services numériques ;
- d'intervenir sur les systèmes pour en garantir le bon fonctionnement ;
- d'informer les utilisateurs en cas de perturbation ou d'intervention planifiée ;
- de signaler à la direction tout comportement suspect ou non conforme ;
- de respecter la confidentialité des données auxquelles ils pourraient accéder dans le cadre de leurs missions.

8. Obligations de signalement

Le signalement rapide des incidents de sécurité est une responsabilité partagée et constitue un élément essentiel de la résilience de l'institution face aux cybermenaces. Tout utilisateur qui constate ou suspecte :

- Un **accès non autorisé** à son compte ou à ses données ;
- La **perte ou le vol** d'un équipement contenant des données institutionnelles ;
- Une **infection** de son équipement par un logiciel malveillant ;
- Une **tentative d'hameçonnage** ou d'ingénierie sociale ;
- Toute autre **anomalie ou incident de sécurité** ;

est tenu de le signaler immédiatement au Centre informatique, selon les modalités de contact définies et communiquées par ce service. La rapidité du signalement est déterminante pour limiter l'impact d'un incident et les éventuelles déclarations auprès des autorités.

9. Sanctions

L'utilisateur qui adopterait des comportements délictueux s'exposerait aux sanctions et poursuites disciplinaires et pénales prévues par les textes législatifs et règlementaires en vigueur.

10. Points de contact

- Pour contacter le Centre informatique (CTI) : cti@ichec.be - 02 739 31 21 **numéro de téléphone à utiliser uniquement en cas d'urgence liée à un incident de cybersécurité**
- Pour contacter le Délégué à la Protection des Données (DPO) : rgpd@ichec.be