

Politique de sécurité informatique de la Haute École Léonard de Vinci

Validée par le Conseil d'entreprise de la HE Vinci du 24 septembre 2021

La présente Politique précise les règles d'utilisations, les droits et les obligations des utilisateurs des systèmes informatiques de la Haute École. Les utilisateurs signataires de la présente Politique s'engagent à respecter les règles ci-dessous et **notamment à ne pas effectuer intentionnellement** des opérations qui pourraient avoir pour conséquences de perturber le bon fonctionnement des ressources informatiques et des réseaux. La Haute Ecole garantit autant que possible aux utilisateurs la mise en place d'un système de sécurité et de protection des données. La Haute Ecole s'engage à mettre en place des outils et un accompagnement adéquats.

Définition

Pour une complète information des obligations découlant de cette politique, il y a lieu d'entendre par :

- Fichier(s) : l'ensemble d'informations ou de données confidentielles ou non, à caractère personnel ou non, qui sont structurées de manière automatisée en tout ou en partie, ou non automatisé en vue de leur utilisation par ou pour la Haute Ecole, dans le cadre de la réalisation de sa mission, principalement pédagogique et de son objet social tel que défini dans les statuts de la Haute Ecole.¹
- Base(s) de données : l'ensemble d'informations ou données, confidentielles ou non, à caractère personnel ou non, organisées en tableau afin d'être facilement consultables, gérables et mises à jour en vue de permettre à la Haute Ecole de réaliser ses missions et son objet social.
- Utilisation à titre privée : s'entend de toute utilisation faite par l'utilisateur à des fins autres que celles définies par sa fonction, sa mission, son contrat ou son statut.
- Système informatique : l'ensemble des moyens matériels et logiciels qui permettent le traitement automatique des informations.

Article 1. Champ d'application

La présente politique s'applique à tout utilisateur du système informatique de la Haute École quelles que soient ses activités.

- Par utilisateur, on entend les membres du personnel administratif, technique et ouvrier, les membres du corps enseignant, la direction, les étudiants de la Haute Ecole ainsi que toute personne à qui la Haute Ecole accorde un accès à titre temporaire aux ressources informatiques.

¹ Cfr statuts de la Haute Ecole : https://www.vinci.be/uploads/HEVinci_Statuts-15-01-2020.pdf

- Par ressources informatiques, on entend notamment le matériel, les logiciels et applications informatiques, l'accès au réseau local et internet, la messagerie électronique, les serveurs et bases de données que la Haute École met à disposition des utilisateurs.

Article 2. Règles d'utilisation des outils informatiques

1. Accès

L'utilisateur doit s'identifier et s'authentifier afin d'accéder aux systèmes informatiques. En aucun cas, il ne peut usurper l'identité d'autrui, agir de façon anonyme ou céder ses droits à un tiers.

L'utilisateur s'engage dès lors à :

- ne pas divulguer ses codes d'accès. Il est entièrement responsable de l'utilisation qui en est faite.
- ne pas utiliser les informations d'authentification d'un autre utilisateur, ni chercher à les connaître.
- ne pas accéder intentionnellement, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- ne pas tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'autorisation explicite.
- verrouiller sa session sur son poste de travail, en cas d'absence, même momentanée.
- ne pas prendre connaissance d'informations confidentielles ou non, détenues par d'autres utilisateurs, et qui ne lui ont pas été adressées, quand bien même l'autre utilisateur ne les aurait pas protégées.
- ne pas tenter d'intercepter des communications entre tiers, en violation du secret de la correspondance notamment.
- ne pas consulter ou conserver des données auxquelles il n'est pas autorisé d'accéder, quand bien même il en aurait pris connaissance accidentellement.

2. Confidentialité

Toute information collectée et contenue dans les fichiers et les bases de données exploitées par l'établissement a un caractère confidentiel (cfr article 6).

L'utilisateur s'engage à préserver la confidentialité des informations, fichiers et bases de données de la Haute Ecole. Il s'engage à prendre toutes les précautions nécessaires pour éviter que ne soient divulguées de son fait ou du fait de personnes dont il a la responsabilité, ces informations confidentielles.

3. Comptes informatiques – messagerie électronique

La Haute École met à la disposition des utilisateurs un compte informatique professionnel nominatif lui permettant d'émettre et de recevoir des messages. L'utilisation de ce compte informatique relève de la responsabilité de son détenteur.

Son utilisation est interdite sur des sites internet sans rapport avec son activité professionnelle ou d'apprentissage. L'aspect nominatif de l'adresse électronique ne retire en rien le caractère professionnel de la messagerie.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature ; il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques...).

Les messages électroniques reçus font l'objet d'un contrôle automatique antiviral et anti-spam. L'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage...), en respectant notamment un comportement normalement vigilant, tel qu'énoncé dans la présente². Si l'utilisateur a un doute sur la nature d'un message, il peut dans ce cas le signaler au service informatique.

Afin de préserver le bon fonctionnement du service de messagerie, la transmission de messages électroniques peut être limitée à un nombre restreint de destinataires. De même, la taille, le nombre et/ou le type des pièces jointes peuvent être limités pour éviter l'engorgement ou la dégradation du système de messagerie.

Les données (en ce compris les documents et informations) contenues dans la boîte électronique sont conservées durant toute la mise à disposition de l'adresse, excepté si l'utilisateur les efface lui-même. Dès la fin de la mise à disposition de l'adresse électronique, les données seront effacées.

La procédure d'effacement des données et de suppression du compte, de l'adresse électronique et de la boîte électronique est réalisée, par la Haute école, comme suit :

1. Désactivation du compte de l'utilisateur dans le logiciel de gestion administrative de la Haute École, (notamment : Pro-éco, Pénélope),
2. Suppression du compte dans le service centralisé d'identification et d'authentification, (ou l'Active Directory),
3. Suppression de l'adresse électronique et de sa boîte auprès du fournisseur de l'adresse, (notamment : Office365).

En toutes circonstances, les adresses électroniques seront supprimées³ :

1. Pour le personnel, dans un délai maximum d'un (1) an après la fin de la relation de travail et ce indépendamment des modalités de la relation ou de fin de la relation de travail. Des délais plus courts peuvent être individuellement convenus.
2. Pour les étudiants qui quittent la Haute Ecole, suppression annuelle des comptes durant le mois d'avril.

4. Internet

L'accès Internet mis à disposition permet de consulter tous types de sites présentant un lien direct et nécessaire avec l'activité scolaire ou professionnelle de l'utilisateur.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites Internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne mettant pas en cause l'intérêt et la réputation de l'établissement, est admise.

La Haute École se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités.

² Voir l'intranet du service informatique gestion de la boîte mail | [Mon courrier \(sharepoint.com\) Sécurité \(sharepoint.com\)](#)

³ Voir l'intranet du service RH/informatique [Durée de validité \(sharepoint.com\)](#)

Le contrôle sera alors effectué en présence d'une personne de confiance.

Les utilisateurs se doivent d'adopter un comportement vigilant, éthique et respectueux lors de l'utilisation des réseaux sociaux, des blogs, qu'ils soient professionnels ou non professionnels.

Il est rappelé que le Code pénal, en particulier les articles 443 et suivants relatifs aux infractions contre l'honneur (diffamation, calomnie, injures, etc.) est applicable également sur les réseaux sociaux.

L'utilisation du/ des réseau(x) sans fil (wifi) et des supports mobiles fera l'objet d'une attention particulière des utilisateurs, qui mettront tout en œuvre pour assurer un niveau de sécurité technique et organisationnelle adéquat pour éviter toute contamination, altération et mise en danger de l'infrastructure informatique de la Haute école.

5. Téléchargement

Le téléchargement de logiciels ou d'œuvres protégées, doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis au livre XI du Code de droit économique⁴ et doit être fait dans le cadre d'usages professionnels.

La Haute Ecole se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système informatique, codes malveillants, programmes espions...).

6. Utilisation à titre privé

L'utilisation du système informatique à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. L'espace utilisé ne doit pas occuper une part excessive des ressources.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur. Par exemple, le téléchargement illégal, la détention, diffusion et exportation d'images à caractère pédophile, ou la diffusion de contenus à caractère raciste ou antisémite sont interdits.

Article 3. Signalement au service informatique

L'utilisateur s'engage à signaler le plus rapidement possible au service informatique tout logiciel ou dispositif suspect ainsi que toute perte, tout vol ou toute compromission suspectée ou avérée :

- d'un équipement stockant des données professionnelles ;
- de ses informations d'authentification (identifiant, mot de passe, code pin, etc.).

Tout signalement doit être effectué dans les meilleurs délais et au plus tard dans les 24 heures (un jour ouvrable) à l'adresse courriel suivante : support@vinci.be

Article 4. Gestion des absences et des départs

Lors de son départ ou d'une absence prolongée, l'utilisateur doit remettre tous les documents professionnels indispensables à la continuité du service à son (sa) responsable ou lui permettre d'y accéder⁵. Dans le cas où l'utilisateur est dans l'incapacité de fournir les documents, son (sa) responsable peut demander au service informatique selon un protocole précis d'accéder à tous les documents et informations professionnels en cas d'absolue nécessité (cfr article 7).

⁴ <https://www.ejustice.just.fgov.be/eli/loi/2013/02/28/2013A11134/justel>

⁵ Cfr article 2.1 sur l'utilisation du mot de passe.

Il est recommandé à l'ensemble des membres du personnel d'utiliser des outils de travail partagé qui facilitent la collaboration et la mise à disposition des documents de manière adéquate pour les collègues et qui permettent d'éviter le recours aux procédures décrites ci-dessus.
En cas de départ, l'utilisateur doit restituer au service de l'informatique, les matériels (ordinateurs portables, téléphones, disques durs externes, clés USB...) mis à sa disposition par l'établissement.

Article 5. Respect de la propriété intellectuelle

La Haute École rappelle que l'utilisation de ses ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

L'utilisateur s'engage à ne pas reproduire, copier, diffuser, modifier ou utiliser des créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits et en indiquant les sources adéquatement.

Article 6. Respect du Règlement Général sur la Protection des Données

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement de données à caractère personnel, conformément au Règlement Général sur la Protection des Données (RGPD) entré en vigueur le 25 mai 2018⁶.

Toute création de fichiers comprenant des informations à caractère personnel 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 le règlement général sur la protection des données et à la charte vie privée.

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement le référent à la protection des données de la Haute École qui prendra les mesures nécessaires au respect des dispositions légales. La communication de données à caractère personnel doit être sécurisée, c'est-à-dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurées.

En outre, 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 systèmes d'information. Ce droit s'exerce auprès du service informatique ou du service du personnel de la Haute Ecole.

Article 7. Traçabilité et contrôles

Les services informatiques disposent d'outils techniques pour procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place. La Haute École informe l'utilisateur que les systèmes informatiques sont surveillés et contrôlés dans le respect de la législation applicable, à des fins de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité, de détection des abus et fraudes.

Toutes les tentatives d'accès infructueuses, activités suspectes et tentatives d'attaques sont enregistrées et envoient des alertes de sécurité au service informatique.

Les services informatiques peuvent procéder périodiquement à des contrôles des fichiers de journalisation (appelés également « journaux » ou « logs ») qui recensent toutes les connexions et

⁶ Référence au journal officiel UE <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679>

tentatives de connexions aux systèmes informatiques. Ces fichiers comportent au minimum les données suivantes : date, identifiant et type d'événement.

Ces fichiers de journalisation sont conservés au maximum douze mois selon la réglementation applicable au type de données conservées.

Article 8. Sanctions

Outre les peines prévues par les dispositions pertinentes de la réglementation en vigueur et applicable à l'infraction commise, le non-respect de la présente Politique peut donner lieu à l'application des procédures de sanctions suivantes :

- le responsable hiérarchique sur avis du service informatique peut retirer, de manière provisoire ou définitive, le droit d'accès à certaines ressources informatiques et/ou réseaux informatiques. Le membre du personnel concerné peut adresser un recours auprès de la Direction-Présidence via l'envoi d'un écrit dans les 14 jours calendrier. Il peut être accompagné dans la démarche par une personne de son choix.
- la direction de la Haute Ecole peut initier une procédure disciplinaire ;
- la direction de la Haute École peut déposer une plainte auprès de la police, engager une action en justice et réclamer des dommages et intérêts dans les limites que lui accorde la loi.

Article 9. Entrée en vigueur de la Politique

La présente Politique remplace tous documents relatifs à l'utilisation des systèmes informatiques de la Haute Ecole. Elle est applicable à compter du 24 septembre 2021 après avis du Conseil d'entreprise du 24 septembre 2021. Elle est annexée au règlement de travail de la Haute Ecole ainsi qu'au règlement général des études.
