



INTÉGRITÉ
CONFIDENTIALITÉ
DISPONIBILITÉ



L'INFORMATION,
une question de sécurité

L'École est déterminée et s'engage à gérer avec efficacité les risques à la sécurité de l'information.

À cette fin, l'École s'est dotée d'une politique de sécurité de l'information et a fait l'embauche d'un conseiller à la sécurité de l'information.

Cette personne est responsable de coordonner la mise en œuvre de cette politique et de sensibiliser la communauté HEC Montréal à la sécurité de l'information.

NOUVEAU site Web

hec.ca/dti/securite

Venez consulter notre site Web pour prendre connaissance :

- de la politique de sécurité de l'information,
- d'informations, de trucs et d'astuces,
- de notre campagne de sensibilisation,
- de la foire aux questions.

Des RAISONS

pour nous consulter ?

- Vous désirez des conseils en sécurité.
- Vous voulez confirmer l'existence ou le bon fonctionnement d'une mesure de sécurité.
- Vous avez besoin de formation sur la sécurité de l'information.

Votre POSTE DE TRAVAIL

- Gardez les mécanismes de protection tels que l'anti-virus, actifs en tout temps.
- Maintenez à jour tous vos logiciels notamment votre système d'exploitation.
- Sécurisez votre portable avec un câble de sécurité.

INTÉGRITÉ • CONFIDENTIALITÉ • DISPONIBILITÉ

COMMUNIQUEZ avec nous :

Sécurité de l'information – Direction des technologies de l'information – HEC Montréal

Marc-André Drapeau Courriel : **securite-info@hec.ca** Téléphone : **514 340-7039**

Site Web : **hec.ca/dti/securite/**

MOT DE PASSE AUTHENTIFICATION MENACE FRAUDE

EXAMEN NOTE PÉDAGOGIQUE SECRET

DISFONCTIONNEMENT CODE SOURCE

BIOMÉTRIE

VULNÉRABILITÉ

MENACE DISPONIBILITÉ

DOSSIER ACADÉMIQUE

NUMÉRO D'ASSURANCE SOCIAL

CHEVAL DETROIS INTÉGRITÉ

SALAIRE RENSEIGNEMENT PERSONNEL

CLÉ FAILLE CONTINUITÉ DES AFFAIRES

CONFIDENTIALITÉ

DOCUMENT PAPIER

CHIFFREMENT SABOTAGE PRÉVENTION DÉTECTION

DISSUASION RÉACTION CONFINEMENT NOTES VERS

VIRUS PLAN DE RELÈVE IDENTIFICATION ANTIVIRUS

LISTE D'ACCÈS JOURNALISATION MALVEILLANCE

GARDE BARRIÈRE VENGEANCE CANULAR INCIDENT

ÉVALUATION CARTE À PUCE NUMÉRO D'EMPLOYÉ

PERTE DE RÉPUTATION DOCUMENT ÉLECTRONIQUE

INFORMATION

Votre MOT DE PASSE

- Le mot de passe est une information personnelle et sensible et doit être confidentiel et secret. Il ne faut pas divulguer son mot de passe.
- Utilisez un logiciel de gestion des mots de passe afin de ne pas les enregistrer sous une forme non protégée. Par exemple : évitez d'écrire son mot de passe sur un « post-it » ou de l'archiver dans un fichier non protégé.

- Changez votre mot de passe temporaire dès la première utilisation.
- Dissociez vos mots de passe pour le travail de ceux de vos services personnels.
- Choisissez un mot de passe de qualité. Consultez notre foire aux questions pour en apprendre davantage sur les mots de passe.

hec.ca/dti/securite/faq

CAPSULE vidéo

Consultez nos capsules vidéo. (5 minutes)

hec.ca/dti/securite/video



Un mot de passe de **QUALITÉ** se définit comme suit :

FACILE À MÉMORISER et DIFFICILE À DEVINER

- Composé d'au moins 8 caractères incluant majuscule, minuscule et chiffre.
- Indépendant de toutes informations personnelles faciles à deviner ou à obtenir : évitez d'utiliser un nom, un numéro de téléphone et une date d'anniversaire.
- Blindé d'une attaque par dictionnaire : évitez d'utiliser un mot du dictionnaire.

Zone FSC



Utilisez un logiciel de gestion **DES MOTS DE PASSE**

- Un logiciel de gestion des mots de passe enregistré pour vous vos mots de passe.
- Il y a plusieurs produits disponibles sur le marché, dont certains sont gratuits et sécuritaires. Consulter notre site Web. hec.ca/dti/securite
- Demandez au centre d'assistance technique de vous installer un logiciel de gestion des mots de passe.

L'INFORMATION,
une question de sécurité