CYBER RÉFLEXES

SÉCURISER LES DONNÉES DE RECHERCHE

1 PROTÉGEZ LES DONNÉES SENSIBLES

La gestion des données sensibles exige une protection maximale, laquelle passe par le chiffrement et le stockage dans des infrastructures sécurisées et conformes aux meilleures pratiques de sécurité.

BONNES PRATIQUES

- Identifiez et classez les données sensibles selon leur niveau de confidentialité. Au besoin, chiffrez les fichiers contenant des informations confidentielles ou liées à la recherche.
- Stockez vos données sensibles dans des serveurs sécurisés ou des services infonuagiques conformes aux normes de sécurité ULaval (Microsoft 365, Azure, AWS, etc.).

2 GÉREZ LES ACCÈS

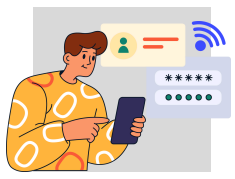
En limitant l'accès aux informations sensibles ou critiques à des personnes autorisées, vous assurez une protection supplémentaire contre des intrusions potentielles.

BONNES PRATIQUES

- Mettez en place des contrôles d'accès stricts tels que l'authentification multifactorielle (AMF).
- Attribuez des droits et des niveaux d'accès adaptés aux différentes personnes utilisatrices: co-chercheurs et co-chercheuses, membres d'une équipe de recherche, étudiants et étudiantes, etc.

3 SÉCURISEZ LE PARTAGE DES DONNÉES

Dans un cadre de collaborations, le partage sécurisé des données de recherche est primordial pour éviter la fuite d'informations confidentielles.

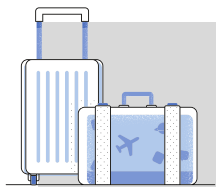


BONNES PRATIQUES

- Chiffrez les communications, les courriels et les transferts de fichiers.
- Utilisez des plateformes sécurisées et approuvées pour partager des données de recherche (ex. : services infonuagiques certifiés, VALERIA, etc.).

4 REDOUBLEZ DE VIGILANCE LORS DES DÉPLACEMENTS

Les voyages ou le télétravail peuvent accroître les risques pour la sécurité des données. Il importe d'utiliser des appareils et des connexions sécurisés pour protéger vos recherches où que vous soyez.

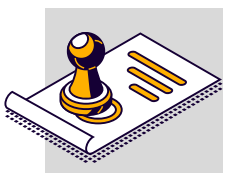


BONNES PRATIQUES

- Évaluez les risques de l'utilisation de vos appareils en fonction de l'endroit où vous allez et du contexte dans lequel vous vous trouverez.
- Assurez-vous d'utiliser des appareils sécurisés, appartenant à votre organisation et dont les logiciels sont à jour.
- Utilisez un réseau privé virtuel (VPN) et l'authentification multifactorielle (AMF).
- Évitez de vous connecter aux réseaux Wi-Fi publics car ils ne sont parfois pas sécurisés ou ont des lacunes par rapport à leurs contrôles de sécurité. Cela peut exposer votre appareil et les systèmes connectés à des cybermenaces.

5 UTILISEZ DES LOGICIELS RECOMMANDÉS

Les solutions technologiques utilisées dans le cadre de vos recherches (logiciels, applications, etc.) doivent être à jour et provenir de sources fiables. Cela évitera de compromettre vos appareils ou l'intégrité, la confidentialité et la disponibilité de vos recherches.



BONNES PRATIQUES

- Utilisez des outils uniquement issus de sources officielles (éditeurs certifiés).
- Activez les mises à jour automatiques pour réduire les risques. Les appareils non à jour sont plus vulnérables aux cyberattaques et aux failles de sécurité.

Plus d'information sur

[Sécurité nationale dans les partenariats en recherche]

Victime ou témoin d'une fraude?
Signalez-le rapidement au Centre de cyberfédense ULaval.

UNIVERSITÉ LAVAL