

Notes pratiques

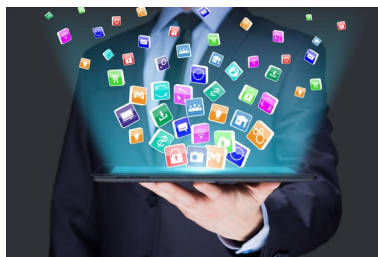
Sur l'accès à l'information et la protection de la vie privée

L'importance de faire vérifier les outils informatiques de tierces parties.

Dans un monde de plus en plus interconnecté, les organismes et les chercheurs s'appuient souvent sur des outils informatiques et des logiciels développés par des tiers parties. Ces outils jouent un rôle essentiel dans divers domaines, tels que la gestion des données, la communication et l'automatisation des processus. Toutefois, leur intégration dans un environnement informatique peut présenter des risques considérables si leur vérification n'est pas effectuée de manière rigoureuse.

Pourquoi est-il important de vérifier les outils informatiques de tierces parties?

- 1- Pour **protéger la sécurité des données**. Les outils développés par des tierces parties peuvent présenter des vulnérabilités qui pourraient être exploitées par des cyberattaquants. Une vérification approfondie permet de détecter ces failles potentielles avant qu'elles ne compromettent les informations sensibles de l'organisme.
- 2- Pour **garantir la conformité réglementaire**. De nombreuses industries sont soumises à des normes et des réglementations strictes en matière de technologie et de données. La vérification des outils informatiques de tierces parties permet de s'assurer qu'elles satisfont à ces exigences, ce qui peut éviter des sanctions juridiques ou financières.
- 3- Pour **évaluer la fiabilité et la qualité**. Un logiciel mal conçu ou instable peut entraîner des interruptions de service, des pertes de données ou des erreurs coûteuses. En vérifiant les outils, un organisme peut éviter d'intégrer des solutions qui pourraient compromettre son fonctionnement.
- 4- Pour **prévenir les conflits de compatibilité**. Les outils informatiques de tierces parties doivent s'intégrer harmonieusement dans l'infrastructure existante d'un organisme. Une vérification permet d'identifier les incompatibilités potentielles qui pourraient conduire à des dysfonctionnements.



La vérification des outils informatiques n'est pas seulement une question de précaution ; elle est une nécessité pour garantir la sécurité, la fiabilité et la conformité des systèmes numériques.

Le Service de technologies de l'information (STI) de l'USB effectue des analyses, des tests approfondis et une surveillance continue des logiciels et des plateformes approuvés à l'USB. Se servir de logiciels non approuvés entraîne de grands risques. De plus, lorsque les données comprennent des renseignements personnels, une évaluation sur l'impact de la vie privée (EIVP) sera amorcée par le Bureau de la protection de la vie privée.

Ignorer ou minimiser l'importance de vérifier les outils informatiques de tierces parties peut avoir des répercussions graves : utilisations de données susceptibles de nuire à la réputation de l'USB, amendes pour non-conformité réglementaire, pertes financières dues à des interruptions de service ou à des erreurs, et manque de confiance de la part de la clientèle et des partenaires.

Puisqu'il vaut toujours mieux prévenir que guérir, il est impératif de ne jamais négliger cette étape essentielle dans la gestion technologique.

Pour toute question concernant la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et la *Loi sur les renseignements médicaux personnels* (LRMP) veuillez communiquer avec Carole Pelchat, coordonnatrice du Bureau de la protection de la vie privée, au poste 398.