Outils de collaboration

Type : Recommandation (pratique)
Référence légale : LGGRI, chapitre G-1.03, 12(6)
Statut : En vigueur
Numéro de référence : P_2020_014
Dernière mise à jour : 2021-05-31
Remplace : • P_2020_004 « Déploiement des outils de collaboration en mode télétravail »

Champ d'application

Organismes (OP) visés à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics (chapitre G-1.03).

Pour chaque outil de collaboration, il est recommandé que les organismes :

- lisent attentivement la politique de confidentialité et les conditions d'utilisation de l'entreprise qui l'offre;
- procèdent à une évaluation des fonctionnalités offertes (par exemple, le transfert et le stockage de fichiers et la capacité d'intégration avec les outils bureautiques en place) et des risques associés à cette utilisation;
- activent les paramètres de sécurité qui assurent la protection des échanges;
- diffusent des règles internes qui en assurent l'utilisation sécuritaire et qu'ils veillent à leur application;
- forment leur personnel quant aux bonnes méthodes de travail;
- offrent un soutien technique à leur personnel, pour une utilisation sécuritaire.

Les organismes doivent également considérer les recommandations du gouvernement américain, par l'intermédiaire du National Institute of Standards and Technology, en ce qui a trait à l'utilisation d'outils de téléconférence :

- Éviter de réutiliser les codes d'accès.
- Utiliser des numéros d'identification personnels différents pour chaque rencontre, s'il y a partage d'information sensible.
- Utiliser une « salle d'attente » pour faire patienter l'invité qui s'apprête à se joindre à l'appel.
- Désactiver les fonctions qui ne répondent pas aux besoins de la rencontre (par exemple, le partage de fichiers).

Infrastructures technologiques Québec (ITQ) est responsable de l'orchestration du déploiement de la plateforme Teams dans tous les organismes publics. Ainsi, il s'assure que les fonctionnalités de sécurité offertes sont correctement déployées et que les échanges sont protégés.

La fiche P_2020_011 Paramètres à appliquer pour sécuriser les environnements Microsoft Office 365 et Microsoft Teams vous donnera plus d'information au sujet de la sécurisation des outils Office 365 et de Teams.

Outils autres que Teams

L'installation d'outils alternatifs repose sur une expertise technologique précise, notamment afin que les différentes fonctionnalités soient configurées de façon adéquate et professionnelle. Il est donc fortement déconseillé au personnel d'installer et de configurer tout outil alternatif sans avoir l'expertise en la matière.

Par exemple, voici certaines recommandations pour une utilisation sécuritaire de la version entreprise de Zoom :

- L'organisme devrait procéder à une mise à jour du produit sur les postes de travail fournis.
- Le personnel doit utiliser le lien de connexion fourni par l'organisme propriétaire des postes de travail.
- Les responsables des rencontres doivent limiter le partage d'écrans des personnes participantes.
- Les responsables des rencontres pourraient exiger un mot de passe aux personnes qui voudraient accéder aux réunions.
- Les responsables des rencontres devraient utiliser les salles d'attente.
- Le personnel doit se déconnecter à la fin de chaque session.
- Le personnel ne doit pas partager l'identifiant ni le lien de la réunion sur des sites publics.

Voir aussi

P_2020_011 Paramètres à appliquer pour sécuriser les environnements Microsoft Office 365 et Microsoft Teams

P_2021_001 Azure et Office 365 – contrôles pour sécuriser la collaboration avec les partenaires

---