# Annexe 3 – Guide en matière de cybersécurité pour les bénéficiaires ultimes

Le présent guide fournit aux bénéficiaires ultimes des ressources ainsi qu'une liste de mesures à prendre pour protéger le personnel, les données, la propriété intellectuelle et les opérations de leurs projets.

## 1. Ressources et recommandations pour l'adoption de normes

- Conseil sur la cybersécurité
- Protection de votre recherche
- Renseignements généraux sur la sécurité de la recherche
- Lignes directrices et outils pour la mise en œuvre de la sécurité de la recherche
- Quelles étapes pouvez-vous prendre pour protéger votre recherche?
- Lignes directrices sur la sécurité nationale pour les partenariats de recherche
- Centre canadien pour la cybersécurité - 10 meilleures mesures de sécurité des TI
- *The 18 CIS Critical Security Controls* (en anglais seulement)
- *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (en anglais seulement)
- *Security and Privacy Controls for Information Systems and Organizations* (en anglais seulement)

## 2. Guide des mesures réalisables


Un cadre de cybersécurité, p. ex. le cadre de cybersécurité NIST, comprend cinq fonctions principales : identifier, protéger, détecter, répondre et récupérer. Pour que votre projet bénéficie d'un plan solide en matière de cybersécurité et de protection de la vie privée, ces cinq fonctions doivent être prises en compte. Nous encourageons les principaux chercheurs affectés au projet à examiner le cadre de cybersécurité NIST ou un cadre similaire avant de ne mettre en œuvre un plan de cybersécurité pour leurs projets. Les principaux conseils et les meilleures pratiques pour protéger l'équipe responsable du projet, les résultats de recherche, les données et la propriété intellectuelle sont les suivants :

1. Sécurisez votre projet dès sa conception!
   Lorsque vous planifiez votre projet et ses différentes étapes, incluez également les objectifs de cybersécurité. Par exemple, (1) pour les actifs du réseau, déterminez le besoin d'authentification multifactorielle dès le début et mettez-la en œuvre le plus tôt possible; (2) mettez en œuvre un contrôle d'accès solide, réduisez les privilèges d'accès des utilisateurs et empêchez les membres du projet d'installer sans autorisation des logiciels sur leurs appareils ou sur les appareils utilisés pour la réalisation du projet; (3) définissez le rôle et les

responsabilités en matière de gestion des incidents et concevez un plan de reprise solide.

2. Établissez et appliquez une politique de sécurité
   Cette approche consiste notamment à informer tous les membres de l'équipe des pratiques comportant des risques comme le partage des mots de passe et à réglementer les appareils mobiles qu'ils peuvent utiliser.

3. Installez des outils de sécurité
   Utilisez des outils et des technologies antivirus et anti-maliciels fiables pour protéger vos ordinateurs, vos routeurs, vos commutateurs et vos appareils intelligents. Vous devez installer ces logiciels sur chaque appareil utilisé dans le cadre du projet. Ces outils analysent le trafic et empêchent les employés d'accéder à des sites malveillants. Ils renforcent la dimension cybersécuritaire de votre projet, et ce, à peu de coûts. Consultez de nombreux avis en ligne pour choisir les outils adaptés à votre projet.

4. Chiffrement des données
   Chiffrez les renseignements de nature délicate du projet et les renseignements personnels sur tous les appareils. Idéalement, vous devriez utiliser des systèmes d'exploitation qui offrent le chiffrement en plus des solutions infonuagiques de tierces parties.

5. Réseaux privés virtuels (RPV)
   Adoptez un RPV sécurisé, qui chiffre les données et modifie la localisation et l'adresse IP. Cette mesure est nécessaire lorsque les membres de votre équipe de projet travaillent à distance et ont besoin d'accéder à l'infrastructure et aux données informatiques du projet.

6. Formation et sensibilisation
   Les membres de l'équipe de projet constituent une cible parfaite pour les pirates informatiques. En fait, la plus grande menace à la cybersécurité de votre projet est le personnel, les collaborateurs et les utilisateurs externes qui ont accès aux ressources du projet. Sensibilisez l'équipe du projet aux aspects de la sécurité liés à l'utilisation d'appareils à distance, à l'authentification, à la gestion des mots de passe, à l'ingénierie sociale ainsi qu'à l'analyse et à l'atténuation des risques. Par exemple, apprenez-leur à détecter les courriels d'hameçonnage. Organisez des ateliers à intervalles réguliers pour leur rafraîchir la mémoire et les tenir au courant des tendances en matière de cybersécurité. Testez continuellement le comportement des membres de l'équipe de projet pendant le projet et leurs autorisations d'accès aux ressources du projet.

7. Confidentialité des données
   Élaborez et mettez en œuvre un protocole de gouvernance, de droits et de confidentialité des données pour le projet. Si vous utilisez un outil de prise de décision automatisée pour les préférences en matière d'autorisation de données, assurez-vous de la qualité de l'outil et de son algorithme sous-jacent.

8. Utilisation des codes ouverts et des logiciels libres
   Bien que les logiciels libres soient largement utilisés pour stimuler l'innovation, ils doivent être utilisés avec une extrême prudence et uniquement lorsque vous connaissez leurs vulnérabilités, que vous avez remédié à ces vulnérabilités et que vous êtes en mesure d'en atténuer les risques.

9. Mise à niveau et correction fréquente des logiciels
   La plupart des systèmes logiciels sont constamment mis à niveau, non seulement pour des raisons d'efficacité, mais aussi de sécurité. Assurez-vous que les logiciels auxquels vous faites confiance sont à jour en appliquant tous les correctifs de sécurité nécessaires.

10. Sauvegarde
    Les sauvegardes permettent de s'assurer que vos données sont sécurisées, qu'elles peuvent être rapidement récupérées et que vous pouvez reprendre là où vous vous aviez arrêté. Il est recommandé d'adopter une stratégie de sauvegarde 3-2-1, qui consiste à disposer de trois copies de vos données, dont deux locales (mais sur des appareils différents) et une hors site (c.-à-d. une sauvegarde en nuage) et, si possible, chiffrez-les.