Norme relative à l'accès à distance

1.1 Aperçu

Le Partenariat s'engage à protéger son personnel et ses partenaires ainsi qu'à se protéger lui-même vis-à-vis d'actions illégales ou préjudiciables, intentionnelles ou non.

La sécurité de l'accès à distance constitue un enjeu exigeant la participation et l'adhésion de chacun des membres du personnel du Partenariat et de chacun de ses affiliés accédant à ses ressources informationnelles et TI dans le cadre de ses fonctions.

Afin de veiller à ce que les ressources informationnelles et TI du Partenariat demeurent, en tout temps, sécurisées comme il se doit, le présent document définit des contrôles efficaces en matière d'accès à distance. Le Partenariat pourrait, à sa seule discrétion, imposer des directives plus strictes en la matière.

1.2 But

Ce document a pour but de fournir un ensemble de normes minimales en matière de sécurité et de protection des renseignements personnels (ci-après appelé « la norme ») à mettre en œuvre dans le cadre de l'accès à distance.

1.3 Portée

Cette norme est obligatoire et s'applique à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat responsables de la gestion, du paramétrage et de l'administration de l'accès à distance au sein de l'organisation. Elle s'applique également aux membres du personnel, aux consultants et aux sous-traitants qui se connectent aux systèmes d'information du Partenariat à partir d'un appareil quelconque lorsqu'ils sont à l'extérieur des bureaux de l'organisation.

1.4 Normes

i. Lors d'un accès à distance aux ressources informationnelles et TI du Partenariat, l'ensemble des normes et des politiques de l'organisation restent en vigueur. Les utilisateurs doivent

lire et comprendre l'ensemble des politiques et des normes du Partenariat qui les concernent, en particulier celles qui figurent à la fin du présent document.

ii. Les utilisateurs ne peuvent accéder aux ressources informationnelles et TI du Partenariat qu'en utilisant les renseignements de connexion leur ayant été attribués.

iii. Il est strictement interdit aux utilisateurs de stocker des renseignements confidentiels ou à diffusion restreinte, quels qu'ils soient, sur des ordinateurs domestiques ou distants, à l'exception de sauvegardes temporaires de données nécessaires à la conduite de travaux à domicile. Pour les définitions de ce que sont des renseignements confidentiels et des renseignements à diffusion restreinte, les utilisateurs doivent se référer à la Politique de classification des renseignements.

iv. En outre, en tant que mesure de sécurité supplémentaire, l'accès à distance à des renseignements à diffusion restreinte n'est autorisé qu'en utilisant une authentification à deux facteurs.

v. Les utilisateurs doivent s'assurer que l'appareil utilisé pour se connecter à distance aux ressources informationnelles et TI du Partenariat n'est pas simultanément connecté à un autre réseau, à l'exception d'un réseau domestique qu'ils contrôlent intégralement.

vi. Tous les ordinateurs utilisés pour accéder à distance aux ressources informationnelles et TI du Partenariat doivent être sécurisés et maintenus comme suit :

- Des outils de lutte contre les virus, les logiciels espions et les logiciels malveillants, ainsi que des pare-feu, doivent être installés et configurés en vue de protéger les données de l'ordinateur.
- Les logiciels ou les programmes correctifs doivent être installés et mis à jour.
- Les renseignements du Partenariat ne doivent pas être automatiquement sauvegardés dans le nuage.

vii. Lorsqu'une authentification à deux facteurs est requise, le Partenariat utilise un système hors bande qui envoie des mots de passe à usage unique sur le téléphone mobile d'un

utilisateur. Dans ce cadre, il incombe aux utilisateurs ayant recours à une authentification à deux facteurs de :

Ne jamais divulguer les mots de passe à usage unique à un autre utilisateur.

- Ne jamais copier les mots de passe à usage unique sur un support, quel qu'en soit le type.

viii. L'accès à distance aux ressources informationnelles et TI du Partenariat à partir d'un réseau sans fil domestique est autorisé, sous réserve que des mesures de sécurité appropriées soient mises en place. Ces mesures devront, au minimum, consister à :

- Configurer les routeurs sans fil pour une utilisation des protocoles de chiffrement WPA ou WPA2.
- Configurer le SSID (nom de diffusion du réseau Wi-Fi) de sorte qu'il ne contienne aucun renseignement d'identification relatif au Partenariat ou à l'employé, comme le nom de l'organisation, le nom de l'employé ou une adresse.
- Choisir un mot de passe sans fil difficile à deviner et connu des seuls utilisateurs autorisés.
- Interdire les nouvelles connexions sans l'approbation explicite de l'administrateur ou du détenteur du réseau sans fil.

ix. L'accès à distance aux ressources informationnelles et TI du Partenariat à partir de réseaux publics sans fil, notamment Wi-Fi, n'est autorisé que par l'intermédiaire d'une connexion VPN sécurisée et approuvée par le Partenariat. Il s'agit notamment d'accès à partir de lieux publics utilisant des réseaux sans fil non sécurisés, notamment Wi-Fi, comme les cafés Internet. L'accès à distance aux ressources informationnelles et TI du Partenariat à partir d'appareils mobiles n'est autorisé que par l'intermédiaire d'un réseau de données cellulaires, à l'exclusion des réseaux publics Wi-Fi.

1.5 Contrôle de l'application de la politique

En cas de non-respect de cette norme, le Partenariat pourra, sans que cela soit limitatif, prendre les mesures suivantes :

i. Refuser l'accès à ses ressources informationnelles et à ses technologies de l'information.

ii. Mettre en œuvre, pour les fournisseurs indépendants, les consultants ou les sous-traitants, les recours contractuels appropriés, par exemple les dispositions relatives aux manquements au contrat ou à sa résiliation.

iii. Mettre en œuvre, pour le personnel, des mesures disciplinaires pouvant inclure, sans que cela soit limitatif, un avertissement écrit, une suspension avec ou sans traitement ou un licenciement immédiat motivé sans aucun préavis ni autre obligation.

1.6 Définitions

Terme	Définition
Ressources informationnelles et TI	Matériel informatique (y compris les ordinateurs portatifs et de bureau), logiciels, systèmes d'exploitation, supports de stockage, comptes réseau, courrier électronique, accès Internet, portails, passerelles, appareils réseau, appareils mobiles, serveurs, téléphones et systèmes téléphoniques, imprimantes multifonctions, ordinateurs personnels et domestiques connectés au réseau du Partenariat, directement ou par l'entremise d'une connexion VPN, ressources informationnelles (quel que soit le support ou le format), par exemple les renseignements commerciaux ou personnels, ainsi que tout autre élément que le Partenariat pourrait considérer comme une ressource informationnelle ou TI
Utilisateur	Toute personne qui consulte ou utilise les ressources du Partenariat
Accès à distance	Accès aux systèmes du Partenariat depuis l'extérieur de ses locaux

Authentification à deux facteurs	L'authentification à deux facteurs exige deux facteurs indépendants avant que l'accès ne soit autorisé (par exemple un élément détenu par la personne autorisée et un élément qu'elle connaît). L'authentification à deux facteurs comprend généralement : • Un nom d'utilisateur et un mot de passe valides émis et attribués par le Partenariat à une personne. • Un mot de passe ou un NIP envoyé sur l'appareil mobile d'une personne par SMS afin de lui permettre d'accéder à certains renseignements du Partenariat.
Authentification hors bande	L'authentification hors bande désigne un processus dans le cadre duquel l'authentification nécessite deux signaux différents provenant de deux réseaux ou deux canaux distincts. Le concept fondamental sous-jacent à ce type d'authentification est qu'en utilisant deux canaux différents, les systèmes d'authentification sont en mesure de se prémunir contre les tentatives frauduleuses d'utilisateurs ne pouvant avoir accès qu'à l'un de ces canaux.

1.7 Documents connexes

- Politique d'utilisation acceptable
- Politique sur les appareils mobiles
- Politique de sécurité de l'information et des technologies de l'information
- Politique de classification des renseignements
- Norme relative au courrier électronique
- Norme relative aux mots de passe
- Code de conduite RH

Fin du document