Titre :	**Accès reseau confiance zéro (ZTNA)**		
État :	Approuvé	Effective à partir de :	2022-06-20
		Dernière mise à jour :	2022-06-20

Type :	Exigences		
Code du document :	MSSS-EXI-001	Portée :	MSSS et RSSS
Mots clés :	Zero trust; Confiance zéro; ZTNA; Exigence		
Justification :	L'organisation doit assurer la validité de tous les terminaux qui accèdent aux applications et assurer une veille sur ces derniers, qu'ils soient sous sa gestion ou non. Un minimum de règles de sécurité est imposé pour chaque appareil qui doit y répondre pour assurer sa légitimité et son intégrité.		
Lien avec :	Orientation : MSSS-ORI-001 Accès réseau confiance zéro (ZTNA)		

Déclaration :	**La gestion des appareils n'exclus aucun équipement - gérés ou non**
Précisions :	
Les services ZTNA doivent avoir la capacité de prendre en charge aussi bien les appareils appartenant aux employés qu'à l'organisation. Il faut prendre en charge l'accès à la fois par des appareils appartenant à l'organisation (donc gérés) et par des terminaux appartenant aux employés. Des règles minimales de sécurité sont définies pour tous types d'équipements – gérés ou non - afin d'assurer un minimum d'état d'intégrité requis.	

Déclaration :	Le Multifacteur imposé pour tous les utilisateurs
Précisions :	
Minimalement, lors de la première connexion sur un nouvel appareil ou une nouvelle application, le nom d'utilisateur et un mot de passe doivent être associés à un autre facteur d'authentification pour confirmer l'identité de l'utilisateur. Ce deuxième facteur doit être généré - ou reçu - sur un autre canal ou appareil que celui utilisé pour la connexion. L'utilisateur doit saisir ses identifiants et effectuer une seconde action : • Saisie d'un code envoyé par SMS, mail ou généré par une application (OTP) • Validation de la demande d'accès via une application (PUSH) • Utilisation d'un jeton RSA ou de clé d'authentification	

Déclaration :	La détection axée sur les activités
Précisions :	
Des politiques d'accès aux utilisateurs et aux appareils doivent être spécifiques à chaque application. Ainsi la surveillance se matérialise par la définition des activités reconnues et des activités anormales dans les fonctionnalités des services ZTNA. Ces activités sont surveillées en corrélation avec ces politiques d'accès et l'analyse comportementale définies par : • le cadre de gouvernance de la sécurité de l'information de l'organisation; • les détenteurs et les gestionnaires des solutions.	

Déclaration :	Les services ZTNA sont intégrés dans les outils de préventions et de détection en matière de sécurité
Précisions :	
Les services de ZTNA doivent notamment s'intégrer dans les outils de prévention de la perte et fuite de données (DLP), de gestion des appareils mobiles (MDM), de gestion des applications (MAM), ainsi que de surveillance comme des systèmes SIEM et toute autres solutions en la matière.	