Titre :	Exigence encadrant les communications numériques avec les citoyens		
État :	Approuvé	Effective à partir de :	2023-11-21
		Dernière mise à jour :	2023-11-21

Type :	Exigences		
Code du document :	MSSS-EXI-009	Portée :	MSSS et RSSS
Mots clés :	Hameçonnage;Escroquerie en ligne;Cybermenace;Confidentialité;Fuites de données;Usurpation d'identité;Liens cliquables; URL		
Justification :	Dans le but de réduire les risques d'hameçonnage, d'escroqueries en ligne et d'autres cybermenaces, le MSSS et le RSSS s'engagent à ne pas inclure de liens cliquables dans les messageries et courriels destinés aux citoyens. Cette mesure préventive vise à décourager les clics sur des liens potentiellement malveillants qui pourraient se trouver dans des messages frauduleux. De plus, pour protéger davantage la confidentialité des données sensibles des citoyens et réduire les risques de fuites de données et d'usurpation d'identité, il est impératif que les informations personnelles ne soient pas divulguées dans les communications numériques du MSSS et du RSSS.		

Déclaration :	**Les communications numériques aux citoyens ne doivent pas contenir de liens cliquables ni transmettre ou demander des renseignements personnels**
Précisions :	
Les communications numériques envoyées aux citoyens (courriels, messageries, etc.) doivent respecter les règles suivantes : **Confidentialité et sécurité :** • Aucune information sensible ou confidentielle ne doit être transmise. • Toute demande d'informations personnelles est interdite. **Navigation Web :** • Les adresses de ressources Internet (URL) ne doivent pas être incluses dans les messages, qu'elles soient cliquables ou non ou sous forme de codes QR. • Pour orienter les citoyens vers des ressources en ligne, privilégiez des références à des sites connus sans divulguer directement l'adresse URL. Par exemple, conseillez de visiter le site officiel d'un établissement et de naviguer vers la section désirée. **Accès à l'information :** • Encouragez les destinataires à localiser l'URL par eux-mêmes, par exemple en cherchant le site Web du MSSS ou celui du CIUSSS. Des directives précises faciliteront cette démarche. • Recommandez des méthodes de validation de l'expéditeur pour confirmer l'authenticité des messages. **Exceptions :** • Les adresses URL peuvent être transmises en réponse à une action liée à l'authentification spécifiquement initiée par l'utilisateur, comme lors d'un processus de réinitialisation de mot de passe, pourvu que la validité du lien soit temporairement limitée. • Lors d'une interaction directe avec un intervenant, que ce soit en visioconférence ou en personne, il est permis d'envoyer un courriel contenant une URL cliquable, à condition que le citoyen en soit informé au cours de cette interaction et que la validité du lien soit limitée dans le temps.	
Justification :	L'adoption de cette approche : • Réduit les chances que les citoyens soient trompés par des courriels ou des messageries frauduleux; • Permet de se conformer à l'orientation gouvernementale en la matière; • Augmente la confiance dans les communications officielles; • Favorise la vigilance numérique et l'éducation en matière de cybersécurité.
Lien avec :	MSSS-DIR-001 : Directive sur la cybersécurité – extranet RSSS