Exigences en matière d'assurance cybernétique – Fiche d'aide

	Renseignements supplémentaires pour fournir des conseils sur les exigences générales des assureurs :	Exemples pratiques de la manière dont vous ou votre fournisseur de services informatiques pouvez mettre en œuvre cette exigence :	Pour plus d'informations :
4 EXIGENCES DE SÉCURITÉ ESSENTIELLES POUR BÉNÉFICIER DE LA GARANTIE :			
1. Vous effectuez régulièrement des sauvegardes hors lignes ou à froid de données critiques, qui ne seraient pas affectées par un problème survenant dans votre environnement réel, et vous effectuez des tests pour vous assurer que ces sauvegardes sont récupérables.	Il est impératif pour toutes les organisations d'effectuer des sauvegardes régulières de leurs données cruciales et de veiller à ce que ces sauvegardes soient à la fois récentes et récupérables. En agissant ainsi, vous garantissez la continuité des opérations de votre organisation face à divers scénarios tels que les cyberattaques, les suppressions accidentelles, les dommages physiques ou le vol de données. De plus, disposer de sauvegardes actualisées vous protège contre les tentatives d'extorsion de la part de cybercriminels exploitant des logiciels de rançon. Il est recommandé d'effectuer les sauvegardes aussi fréquemment que possible, idéalement quotidiennement, afin de réduire au minimum la perte de données en cas de restauration à partir de la sauvegarde la plus récente.	De nombreuses plateformes intègrent désormais des fonctionnalités de sauvegarde; il est donc judicieux d'explorer les options dont vous disposez déjà. Vous pouvez également envisager une solution de sauvegarde tierce, telle que des plateformes de sauvegarde dans le nuage, ou effectuer vos propres sauvegardes sur des disques externes que vous gardez en lieu sûr, déconnectés de votre environnement principal.	https://www.cyber.gc.ca/fr/orientation/sauvegarder-et-recuperer-vos-donnees-itsap40002

2. Vous utilisez l'AMF (authentification multifacteur) pour l'accès à votre compte de messagerie infonuagique et pour tous les accès à distance à votre réseau.	Les mots de passe ne garantissent plus une sécurité adéquate, surtout pour les services accessibles via le nuage (tels que Microsoft 365, Google Workspace, etc.). Les utilisateurs ont tendance à opter pour des mots de passe faciles à deviner et/ou à les divulguer involontairement par le biais du piratage psychologique. L'authentification multifacteur (AMF) revêt une importance cruciale, car elle rend le vol d'informations beaucoup plus ardu pour les cybercriminels lambda.	L'authentification multifacteur (AMF) ne supprime pas les noms d'utilisateur ou les mots de passe, mais ajoute une couche de sécurité supplémentaire au processus de connexion. Lors de l'accès à des comptes ou des applications, les utilisateurs doivent fournir une preuve d'identité supplémentaire, comme un scan d'empreinte digitale ou la saisie d'un code reçu par téléphone ou via une application mobile. L'AMF est intégrée à la plupart des services basés sur Internet ou dans le nuage, il est donc recommandé de l'activer. En outre, il existe des fournisseurs tiers proposant des services de vérification d'identité via des codes SMS, des codes uniques et même des jetons matériels.	https://www.cyber.gc.ca/fr/orientation/quest-ce-que-lauthentification-multifacteur
3. Vous n'autorisez pas l'accès à distance dans votre environnement sans RPV (réseau privé virtuel).	Les pirates effectuent régulièrement des scans de ports sur l'ensemble d'Internet à la recherche de services d'accès à distance visibles, tels que le protocole RDP (*Remote Desktop Protocol*) de Microsoft. Tout service RDP ouvert est constamment scruté à la recherche de failles. En dissimulant vos services d'accès à distance derrière un RPV, vous bénéficierez d'un niveau de protection élevé contre ces attaques.	Tout comme pour l'authentification multifacteur (AMF), de nombreux fournisseurs tiers offrent des services RPV, et votre propre infrastructure réseau, tels que les routeurs, peut également intégrer cette fonctionnalité, qu'il vous suffit donc d'activer.	https://www.cyber.gc.ca/fr/orientation/les-reseaux-prives-virtuels-itsap80101

	Renseignements supplémentaires pour fournir des conseils sur les exigences générales des assureurs :	Exemples pratiques de la manière dont vous ou votre fournisseur de services informatiques pouvez mettre en œuvre cette exigence :	Pour plus d'informations :
4. Vous organisez régulièrement (au moins une fois par an) une formation de sensibilisation à la cybersécurité, incluant la prévention de l'hameçonnage, à l'intention de tous les individus ayant accès au réseau de votre organisation ou à des données confidentielles/personnelles.	Votre personnel constitue le premier rempart de votre organisation. Ils sont constamment en contact avec des communications électroniques provenant de tiers, exposant ainsi l'entreprise à des risques d'attaques. Bien que les mesures de sécurité techniques telles que les passerelles de messagerie électronique et les logiciels EDR puissent fournir un certain niveau de protection, il est essentiel que les employés soient conscients des risques encourus. La formation les aidera à reconnaître les cybermenaces et, idéalement, à les neutraliser avant qu'elles ne portent préjudice à votre organisation.	Le NCSC (*National Cyber Security Centre*) propose une formation gratuite sur la cybersécurité pour le personnel, incluant un module de lutte contre l'hameçonnage. Par ailleurs, plusieurs fournisseurs tiers offrent une variété de services de formation en cybersécurité. Notre partenaire fournisseur, KnowBe4, propose notamment des formations accessibles à des tarifs préférentiels pour les assurés de Beazley.	https://www.pensezcybersecurite.gc.ca/fr
3 MESURES DE SÉCURITÉ IMPORTANTES : NON REQUISES POUR ÊTRE ADMISSIBLE À L'ASSURANCE, MAIS IMPORTANTES À CONSIDÉRER			
5. Vous appliquez les correctifs critiques et mettez à jour les systèmes dès que possible, et n'utilisez aucun logiciel non pris en charge/en fin de vie (EOL-End of Life).	Chaque plateforme logicielle bénéficie régulièrement de mises à jour, communément appelées « correctifs » ou « patches ». Ces mises à jour peuvent introduire de nouvelles fonctionnalités ou visent à résoudre des problèmes tels que l'instabilité ou des opérations non désirées, susceptibles d'être exploitées par des pirates (vulnérabilités). Étant donné que de nouvelles vulnérabilités sont constamment découvertes et corrigées, l'application des correctifs émis par les éditeurs de logiciels représente une tâche de sécurité routinière qui devrait être au cœur de la posture de cybersécurité de base de toute organisation.	La plupart des systèmes d'exploitation permettent une mise à jour ou un correctif très simple. Pour les autres logiciels, veuillez consulter le site web du fournisseur concerné ou d'autres canaux pour vous assurer d'être informé des correctifs et des versions critiques. Les fournisseurs annoncent généralement lorsque leurs logiciels ne sont plus pris en charge ou qu'ils sont en fin de vie. Il est impératif de prendre connaissance de ces communications afin de pouvoir remédier à la situation.	https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientation-gestion-rustines.html

	Renseignements supplémentaires pour fournir des conseils sur les exigences générales des assureurs :	Exemples pratiques de la manière dont vous ou votre fournisseur de services informatiques pouvez mettre en œuvre cette exigence :	Pour plus d'informations :
6. Vous examinez les courriels entrants à la recherche de pièces jointes et/ou de liens malveillants.	Le courrier électronique demeure la principale forme de communication électronique pour la plupart des organisations, ce qui en fait une cible de choix pour les pirates cherchant à compromettre votre personnel. Les passerelles de messagerie électronique jouent un rôle crucial en protégeant les collaborateurs des menaces associées aux courriels, telles que le pourriel, les virus et les attaques par hameçonnage, en filtrant les messages potentiellement malveillants avant qu'ils n'atteignent leur boîte de réception.	En isolant les courriels malveillants dans une zone de quarantaine ou en bloquant ces messages ou leurs expéditeurs, une passerelle de messagerie électronique devrait considérablement réduire le nombre de tentatives de compromission réussies des informations d'identification de l'utilisateur, tout en abaissant le risque d'exposition des données sensibles. La plupart des plateformes de messagerie offrent des fonctionnalités de filtrage et de quarantaine de base, il est donc essentiel de les activer. Idéalement, vous pouvez également envisager des fournisseurs spécialisés en passerelles de messagerie électronique pour des solutions plus avancées.	https://www.cyber.gc.ca/fr/orientation/ne-mordez-pas-lhamecon-reconnaitre-et-prevenir-les-attaques-par-hameconnage
7. Vous protégez tous vos appareils à l'aide d'un logiciel antivirus, antimaliciel et/ou de protection des points d'extrémité.	Les antivirus, les antimaliciels et les systèmes de détection et de réponse (EDR) sont des logiciels conçus pour détecter, bloquer et/ou supprimer les logiciels malveillants présents sur les appareils. Les outils EDR modernes sont souvent intégrés à une plateforme de journalisation, permettant aux organisations d'analyser l'ensemble de leur parc informatique afin d'identifier les modèles ou tendances émergents susceptibles de signaler la présence d'un pirate dans leur environnement. Ces outils jouent un rôle crucial dans la stratégie de cybersécurité de toute organisation, car ils visent à éliminer proactivement les logiciels malveillants, une fonction que les pare-feu traditionnels ne peuvent pas assurer.	Il existe de nombreux outils disponibles à cet effet, et le lien suivant fourni par le NCSC offre des conseils sur la sélection, la configuration et l'utilisation d'antivirus ainsi que d'autres logiciels de sécurité pour les téléphones intelligents, les tablettes, les ordinateurs portables et les ordinateurs de bureau.	https://www.getcybersafe.gc.ca/en/blogs/how-évaluez-le-logiciel-antivirus-et-choisissez-le-bon-vous