1.0 GESTION DES DISPOSITIFS RÉSEAU DE TO

1.1 Les dispositifs réseau de TO doivent utiliser un fournisseur, un modèle et une configuration sécurisée.
1.2 Les dispositifs réseau de TO ne peuvent pas être installés sur les réseaux de TO par une personne ou un groupe en dehors de l'équipe administrative, à moins d'une autorisation du client.
1.3 Les dispositifs réseau de TO doivent être corrigés ou mis à jour en réponse aux vulnérabilités de sécurité, le cas échéant.
1.4 Les configurations ou les modifications des dispositifs réseau de TO doivent être consignées, examinées, mises à l'essai et déployées conformément à la politique de gestion du changement en matière de TI.
1.5 La documentation relative aux réseaux de TO et aux dispositifs réseau doit être classifiée, stockée et traitée conformément aux politiques des administrations régionales.
1.6 Toute la documentation relative au réseau de TO contenant des renseignements précis sur la configuration et le traitement du réseau doit être classifiée comme « Confidentielle ».
1.7 Les réseaux de TO doivent être disponibles pour une évaluation indépendante par des évaluateurs/vérificateurs internes/externes.

2.0 CONFIGURATION DES DISPOSITIFS RÉSEAU DE TO

2.1 Les dispositifs réseau de TO doivent se trouver sur une plateforme matérielle dédiée sur laquelle seuls les logiciels ou les services essentiels d'exploitation de réseau sont installés et exécutés.
2.2 S'il y a lieu, les dispositifs réseau de TO doivent être conçus de manière à offrir une grande disponibilité et des capacités de reprise des activités après sinistre pour répondre aux exigences établies en matière de réseau et de niveau de service opérationnel.
2.3 Les dispositifs de réseau de TO ne doivent pas partager de ressources informatiques avec d'autres applications ou services, sauf pour permettre des contrôles de sécurité comme la surveillance et l'analyse de la sécurité.
2.4 Les dispositifs réseau de TO doivent prendre en charge Zabbix ou d'autres outils approuvés par les TI aux fins de surveillance du trafic réseau et de la sécurité.
2.5 Les mots de passe par défaut des dispositifs réseau de TO doivent être modifiés avant l'installation et le déploiement, selon les instructions de BGIS.
2.6 Les dispositifs réseau de TO doivent maintenir leur configuration et leurs paramètres de sécurité, ainsi que les contrôles d'accès pendant un processus de réinitialisation ou de redémarrage, ou lorsqu'un dispositif réseau échoue alors qu'il est transféré à un dispositif de sauvegarde.
2.7 Les dispositifs réseau de TO doivent être configurés pour transmettre des données d'événements de sécurité au système de gestion des informations et des événements de sécurité afin de permettre la détection des incidents de sécurité et d'enclencher des procédures de réponse aux incidents.
2.8 Les renseignements sur la configuration des dispositifs réseau de TO doivent être effacés de façon sécuritaire avant la mise hors service et l'élimination.
2.9 Les dispositifs réseau de TO doivent être renforcés pour veiller à ce que l'accès physique local nécessite une authentification (par exemple : veiller à ce que la connexion de la console nécessite un mot de passe et désactiver toute connexion auxiliaire comme USB).

3.0 ACCÈS À LA GESTION DES DISPOSITIFS RÉSEAU DE TO

3.1 L'accès aux dispositifs réseau de TO doit être approuvé uniquement pour le personnel autorisé.
3.2 Les droits d'accès et les comptes utilisateur aux dispositifs réseau de TO doivent être certifiés au moins deux fois par an et les artéfacts de vérification doivent être stockés en toute sécurité.

3.3 L'accès aux dispositifs réseau de TO et aux systèmes de gestion de réseau doit être immédiatement révoqué lorsqu'un administrateur change ses responsabilités de travail. Tous les mots de passe de l'administrateur réseau et des services doivent également être réinitialisés.

3.4 L'accès aux segments de gestion de réseau de TO pour les dispositifs réseau de BGIS doit se faire sur un réseau sécurisé distinct. L'accès de la direction aux dispositifs réseau de TO ne doit pas être autorisé à partir d'un réseau non sécurisé (p. ex., à partir d'Internet).

3.5 Dans la mesure du possible, l'accès aux dispositifs réseau de TO pour gérer ceux-ci doit utiliser l'authentification multifactorielle.

3.6 L'accès aux dispositifs réseau de TO et au système de gestion de réseau à l'aide de Telnet, FTP ou d'autres protocoles non chiffrés est interdit.

4.0 SÉCURITÉ DU PÉRIMÈTRE DE RÉSEAU DE TO

4.1 Le cas échéant, les dispositifs réseau de TO doivent avoir des capacités de traitement intégré de données et doivent être activés pour tous les flux de trafic, à l'exception du trafic de type balayage autorisé de BGIS.

4.2 L'équipement du réseau de TO doit être disponible pour une évaluation indépendante par l'audit interne.

4.3 Le périmètre de réseau de TO doit veiller à ce que toute connexion en destination et en provenance d'Internet ou à tout réseau non sécurisé des réseaux de TO de BGIS passe par des passerelles réseau approuvées. La passerelle de TO doit être la seule passerelle disponible entre les réseaux locaux de TO et les zones non sécurisées.

4.4 Le périmètre du réseau doit être configuré pour filtrer le trafic réseau à destination et en provenance d'Internet, en respectant les règles suivantes :

4.5 Règle implicite visant à tout refuser; tout le trafic du réseau de TO est interrompu, à moins que ce ne soit explicitement autorisé.

4.6 Toutes les règles relatives au pare-feu de TO doivent reposer sur le principe du moindre privilège (ne permettre que ce qui est nécessaire au fonctionnement de l'application).

4.7 Les règles du pare-feu de TO doivent être créées de manière à ne pas permettre aux applications tierces de contourner les principes de sécurité (séparation des réseaux) ou les fonctionnalités (accès à distance par l'intermédiaire du réseau privé virtuel [RPV] de TO de BGIS). Exemple : la politique relative à l'Internet sortant doit veiller à ce que les applications de commande à distance (exemple : TeamViewer) ne permettent pas une connexion à distance non autorisée vers le système de TO.

4.8 Tout le trafic traversant le réseau de TO (intrazone ou interzone) doit être chiffré. Pour le chiffrement, TLS est accepté, et la version minimale est TLS 1.2. IPsec est également accepté.

4.9 L'accès à distance à partir d'Internet ou d'autres réseaux externes doit être considéré comme non fiable et doit être authentifié au minimum par une adresse IP source reconnue et confirmée. Ce type de connectivité ne doit être utilisé que par le trafic d'applications.

4.10 L'authentification multifactorielle doit être utilisée lors de la connexion à distance de l'ordinateur d'un utilisateur final à un réseau de TO de BGIS.

4.11 Les sources de trafic des sites Internet et des adresses IP reconnues pour contenir ou lancer des attaques et des maliciels ou pour soutenir des pourriels, des logiciels malveillants, des attaques par déni de service, des plateformes d'attaque réseau, du matériel offensant ou d'autres risques technologiques pour BGIS doivent être bloquées.

4.12 Les réseaux internes du réseau de TO doivent être séparés, le cas échéant. (Exemple 1 : Les dispositifs de TO ne doivent pas se trouver sur le même sous-réseau que les utilisateurs d'entreprise.) (Exemple 2 : Les dispositifs de TO pour l'automatisation des immeubles ne doivent pas être sur le même réseau que les dispositifs de TO pour le système de détection des fuites de l'immeuble.)

4.13 Tous les utilisateurs qui profitent de l'accès à distance au moyen de dispositifs non sécurisés (autres que BGIS) doivent réussir une vérification du profil d'information d'hôte avant de pouvoir se connecter au RPV de TO de BGIS. (Exemple : L'ordinateur de l'utilisateur doit utiliser Windows 10 avec les correctifs Windows les plus récents).

4.14 Le cas échéant, les réseaux de TO doivent avoir une forme de contrôle de l'accès au réseau de niveau 2 ou 3.

5.0 ACCÈS AU RÉSEAU SANS FIL

5.1 Les réseaux de TO utilisent souvent des protocoles d'authentification de base comme WEP ou WPA. Cela est acceptable si ces réseaux suivent le principe du moindre privilège et la séparation du réseau.
5.2 Les réseaux sans fil de TO doivent être masqués si possible.
5.3 Les réseaux sans fil de TO doivent être consacrés à la fonctionnalité du système de TO. Par exemple, les utilisateurs invités du réseau Wi-Fi ne doivent pas partager le réseau sans fil de TO.
5.4 Les utilisateurs locaux des réseaux Wi-Fi doivent avoir une authentification du niveau utilisateur (exemple : RADIUS).

6.0 ADMINISTRATION DE TO

6.1 Les réseaux de TO doivent avoir un utilisateur désigné responsable de l'approbation et de l'autorisation de toute demande liée au réseau de TO respectif. Si un réseau de TO n'a pas d'administrateur désigné, un administrateur doit être affecté avant que les changements puissent être traités.
6.2 L'accès des utilisateurs au réseau de TO doit être entièrement authentifié (avec une autorisation à deux facteurs) et utiliser un répertoire des utilisateurs qui peut être audité et examiné.

7.0 SERVICES INFONUAGIQUES

7.1 Tous les services infonuagiques doivent satisfaire aux exigences minimales suivantes :
7.2 Certifié ISO/IEC 27001 et conforme aux normes ISO/IEC 27017 et ISO/IEC 27018 relatives aux services infonuagiques.
7.3 Résidence des données au Canada, aux États-Unis, Royaume-Uni et l'Australie
7.4 Toutes les données doivent être détruites (lettre de certification signée par le représentant autorisé de l'entreprise) à la résiliation du contrat après le transfert au service de stockage privilégié du client
7.5 BGIS se réserve le droit d'effectuer une évaluation des vulnérabilités en matière de sécurité de toute plateforme infonuagique suggérée et désignée comme pouvant être utilisée. L'évaluation exigera que le fournisseur fournisse les renseignements suivants (sans toutefois s'y limiter) avant l'attribution du contrat ou à tout autre moment pendant la durée du contrat :
7.6 Contrat de licence d'utilisateur final (CLUF)
7.7 Déclarations/politiques en matière de confidentialité
7.8 Politiques sur la résidence et la destruction des données
7.9 Certification ISO/IEC 27001
7.10 Démonstration de l'énoncé de gestion de la sécurité informatique du fournisseur indiquant la conformité à la norme ISO/IEC 27017/27018 pendant la certification ISO/IEC27001 et/ou les évaluations indépendantes des normes de conformité relatives à la norme ISO/IEC 27017/27018.

8.0 EXIGENCES DE BGIS EN MATIÈRE DE PARE-FEU

8.1 Les systèmes et les dispositifs de TO des fournisseurs tiers seront connectés au moyen d'un pare-feu géré par BGIS, conformément à l'architecture suivante. Le fournisseur doit collaborer avec les gestionnaires de réseau de TO de BGIS pour établir une connexion sécurisée au moyen du pare-feu, conformément au schéma suivant.