

Appel de propositions AM004829

**Fourniture d'une solution de télémétrie
véhiculaire, du matériel requis, de la connectivité
et des accès à une plateforme infonuagique
incluant un DCE**

**Cahier de réponses – exigences de
sécurité**

Instructions aux fournisseurs – exigences de sécurité

Ceci est un questionnaire préliminaire afin d’avoir une vision à haut niveau des mécanismes de contrôles en lien avec la sécurité. Les solutions rendues à l’étape finale devront compléter une version plus détaillée du questionnaire pour une évaluation plus approfondie.

Un rapport d’audit de sécurité (de type SOC-2 ou ISO 27000) est requis pour les solutions infonuagiques.

L'absence de ce rapport d'audit pourrait éliminer une solution proposée.

Exigences de sécurité

DOMAINE	RÉPONSE
<p>1 – Gouvernance</p> <p>Décrivez le type de gouvernance mise en place pour la sécurité de l'information?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - Cadre de contrôle - - politiques de cybersécurité - - sensibilisation - - responsable de la cybersécurité - - gestion du risque - - indicateurs/tableaux de bord - - architecture de sécurité - - reddition de compte - 	
<p>2 – Gestion des identités et accès</p> <p>Décrivez les processus et mécanismes mis en place pour gérer les identités et les accès de vos employés, de vos tiers et des utilisateurs de votre solution?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - Modèle de gestion des accès - - imputabilité - - traçabilité - - cycle de vie des comptes - - privilèges élevés - - authentification 2 facteurs - - révision des accès - - fédération d'identités - 	
<p>3 – Sécurité de l'infrastructure</p> <p>Indiquez comment vous maintenez de manière sécuritaire les infrastructures de la solution?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - configuration des infrastructures - - ségrégation des environnements clients - - architecture réseau - - journalisation - - surveillance et détection d'attaques - - gestion des appareils mobiles - 	

DOMAINE	RÉPONSE
<p>4 – Continuité et résilience</p> <p>Décrivez les processus et mécanismes mis en place pour offrir un niveau de disponibilité élevé?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - Politique/plan de sauvegarde - - relève de la solution - - continuité des opérations - - tests des plans de continuité - - sécurité physique - 	
<p>5 – Protection de l'information</p> <p>Précisez les moyens mis en place pour protéger l'information durant tout son cycle de vie?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - Chiffrement en transit - - chiffrement en stockage - - gestion des clés de chiffrement - - support amovible - - ségrégation des environnements (production et autres environnements) - - information en fin de vie (suppression) - 	
<p>6 – Gestion des changements et contrôles applicatifs</p> <p>Indiquez la manière dont vous assurez un haut niveau de sécurité à vos applications et comment vous gérez les changements touchant vos infrastructures et applications?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - Cycle de développement sécuritaire (OWASP, ISO 27034, etc.) - - tests de qualité - - tests de pénétration - - gestion des changements - 	

DOMAINE	RÉPONSE
<p>7 – Gestion des vulnérabilités, incidents et enquêtes</p> <p>Expliquez votre processus de gestion des vulnérabilités, son arrimage avec la gestion des incidents ainsi que la gestion des enquêtes?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - Vigie - - gestion des vulnérabilités - - application des correctifs - - gestion des incidents - - notification d'Hydro-Québec en cas d'incident - - assistance fournie durant une enquête Hydro-Québec - - autorisation pour un balayage de vulnérabilités réalisé par Hydro-Québec - 	
<p>8 – Assurance</p> <p>Décrivez la manière dont vous démontrez à vos clients que vos contrôles de cybersécurité sont bien documentés, en place et efficaces?</p> <p><i>En une phrase maximum par point d'intérêt:</i></p> <ul style="list-style-type: none"> - indépendance de l'auditeur - - crédibilité de l'auditeur - - type de rapport d'audit - - nature des tests (design et/ou efficacité) - - fréquence des audits - portée des contrôles - - portée de l'architecture de la solution - - résultats de l'audit - 	