



POLITIQUE DE SÉCURITÉ DE L'INFORMATION

**QUANTUM JURICOMPTABLE INC.
ET ALIAS^{MC}**

VERSION 1.5 – 14 janvier 2020

TABLE DES MATIÈRES

1.	Historique des modifications	1
2.	Préambule	2
3.	Objectifs	2
4.	Champs d'application	3
5.	Définitions	3
6.	Principes directeurs	4
7.	Rôles et responsabilités	6
8.	Approbation et date d'entrée en vigueur	6

1. HISTORIQUE DES MODIFICATIONS

Version	Date	Auteur	Description
1.1	2017-11-01	Caroline Ménard	▪ Version approuvée
1.2	2017-12-12	Myriam Levesque	▪ Version diffusée sur le site Internet Quantum
1.3	2019-09-24	Sarah-Mary Doyon	▪ Ajout des responsabilités des utilisateurs à la section 7.
1.4	2019-11-04	Dominique Vachon	▪ Précisions apportées dans les principes directeurs
1.5	2020-01-14	Sarah-Mary Doyon	▪ Précisions dans les rôles et responsabilités

2. PRÉAMBULE

La présente politique (ci-après « la Politique ») précise les objectifs, les principes, et les rôles et responsabilités garantissant la sécurité de l'information et des actifs informationnels recueillis, traités et conservés par Quantum Juricomptable inc. (ci-après « Quantum ») et par Alias, Ligne de signalement inc. (ci-après « ALIAS^{MC} ») dans l'exercice de leurs fonctions.

3. OBJECTIFS

La Politique a pour but d'affirmer l'engagement de Quantum et d'ALIAS^{MC} face à leurs obligations à l'égard de la sécurité de l'information, afin d'assurer la disponibilité, l'intégrité et la confidentialité de celle-ci.

Cette politique a aussi pour but de démontrer la position claire de Quantum et d'ALIAS^{MC} à mettre en place les mesures de sécurité nécessaires à la protection de leurs actifs informationnels, ainsi que ceux de leurs clients respectifs. Elle a été élaborée conformément aux engagements de Quantum et d'ALIAS^{MC} envers leur clientèle respective ainsi qu'avec le cadre légal et réglementaire applicable.

Elle énonce également les orientations stratégiques que Quantum et ALIAS^{MC} se donnent en matière de sécurité de l'information et définit les rôles et responsabilités des intervenants en cette matière.

4. CHAMPS D'APPLICATION

La Politique s'applique aux actifs informationnels, aux intervenants et aux activités suivantes :

Actifs informationnels

Cette politique vise toute information recueillie, détenue ou utilisée par Quantum ou ALIAS^{MC}, peu importe sa nature, sa forme, son support et son emplacement. Elle s'applique à tout le cycle de vie des actifs informationnels.

Intervenants

Cette politique s'adresse à l'ensemble du personnel, peu importe son statut, et toute personne physique ou morale qui, à titre d'employé, de contractuel, de mandataire, de partenaire ou de fournisseur (ci-après « les utilisateurs »), accède, utilise ou gère des actifs informationnels de Quantum ou d'ALIAS^{MC}.

Activités

Cette politique porte sur toutes les activités de Quantum et d'ALIAS^{MC}. Elle s'applique à la collecte, consultation, production, hébergement et destruction des actifs informationnels, et ce, peu importe le lieu où les activités sont conduites. Elle prend également en considération les exigences de sécurité pertinentes dans le cadre des activités de développement, d'exploitation, de maintenance et d'évolution de l'application ALIAS^{MC} et de son infrastructure technologique.

5. DÉFINITIONS

Actifs informationnels

Les actifs informationnels comprennent l'ensemble des informations, numériques ou non, détenues par Quantum ou ALIAS^{MC}. Ils englobent aussi toutes les composantes technologiques utilisées en rapport avec l'information.

Confidentialité

Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes désignées et autorisées par Quantum ou ALIAS^{MC}.

Disponibilité

Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Intégrité

Propriété d'une information de ne pas être détruite ou altérée de quelque façon, sans autorisation, et d'être conservée sur un support qui lui procure la stabilité et la pérennité voulue.

Sécurité de l'information

Processus visant à protéger l'ensemble de l'information peu importe son support, et ce, en fonction de la valeur de l'information, des risques et des impacts relatifs à la disponibilité, à l'intégrité et à la confidentialité de l'information. Ce processus fait appel à une approche globale et intégrée des aspects humains, juridiques, organisationnels, technologiques et éthiques.

Cycle de vie

Durée de vie de l'information, de sa création ou son acquisition, en passant par son traitement, stockage, transmission, utilisation, jusqu'à sa restitution, destruction ou archivage.

Infrastructure technologique

Ensemble des installations, des équipements et des logiciels nécessaires à l'emploi des technologies de l'information et permettant l'accès à l'information.

6. PRINCIPES DIRECTEURS

Les énoncés suivants constituent les orientations organisationnelles en matière de sécurité de l'information. Ils précisent le cas échéant les moyens que Quantum et ALIAS^{MC} se donnent pour y parvenir.

Évolution et universalité

Les pratiques et les solutions de la sécurité de l'information retenues sont réévaluées périodiquement en tenant compte des changements dans l'environnement interne et externe de Quantum et d'ALIAS^{MC} et de l'évolution des menaces et des risques. Ces pratiques et solutions respectent les façons de faire et bonnes pratiques reconnues dans l'industrie.

Protection de l'information

L'information détenue par Quantum ou ALIAS^{MC} dans l'exercice de leurs fonctions est protégée, pendant tout son cycle de vie et ce, peu importe le lieu, par des mesures de sécurité appropriées qui assurent sa disponibilité, son intégrité et sa confidentialité. Cela inclut également les mesures nécessaires à la relève et continuité des activités.

Responsabilité et imputabilité des utilisateurs

La protection de l'information s'appuie sur l'engagement continu de tous les utilisateurs. La sensibilisation et la formation à la sécurité de l'information s'avèrent des éléments essentiels. Ainsi, chaque utilisateur a l'obligation de protéger l'information mise à sa disposition et de l'utiliser avec discernement et aux seules fins prévues. Cette imputabilité s'applique aux actifs informationnels, aux processus et aux systèmes sous la responsabilité ou contrôle de Quantum et ALIAS^{MC}, ainsi que ceux délégués à un tiers.

Éthique

Les processus et solutions de la sécurité de l'information sont soutenues par une démarche éthique renforçant la régulation des conduites et la responsabilisation individuelle.

Cohérence des mesures

La gestion de la sécurité de l'information est basée sur une approche cohérente et intégrée qui tient compte des aspects humains, juridiques, organisationnels, technologiques et éthiques. Les investissements en sécurité de l'information sont prévus dans le but de maintenir les risques de sécurité de l'information à un niveau acceptable pour l'organisation.

Gestion des opérations de sécurité et des incidents

La gestion des opérations de sécurité et des processus afférents est essentielle pour assurer la protection des actifs de l'organisation, afin de contrer les principales menaces. Les processus de gestion des incidents et de gestion des vulnérabilités sont en place pour traiter efficacement et rapidement les menaces s'étant matérialisées.

Droit de regard et d'intervention

Quantum et ALIAS^{MC} exercent, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur l'utilisation de ses actifs informationnels.

Sauvegarde et stockage des actifs informationnels

Les actifs informationnels numériques de Quantum et ceux d'ALIAS^{MC} sont sauvegardés sur les plateformes spécifiquement prévues à cet effet. Le matériel informatique et autre fourni par Quantum et ALIAS^{MC} aux utilisateurs désignés fait l'objet d'un suivi. Les documents physiques de Quantum et ALIAS^{MC}, incluant tout document reçu d'un client sont stockés dans les locaux physiques sécurisés prévus à cet effet.

7. RÔLES ET RESPONSABILITÉS

Quantum et ALIAS^{MC} se sont dotés de rôles et responsabilités adéquats pour la gestion de la sécurité de l'information.

De leur côté, les utilisateurs (incluant les employés de Quantum et/ou ALIAS^{MC}, les sous-traitants ALIAS^{MC}, et les sous-traitants aux services d'enquête Quantum) doivent:

- prendre connaissance et s'engager à respecter la politique de sécurité de l'information, les codes de conduite et toutes autres directives touchant la sécurité de l'information, incluant la présente documentation des Rôles et responsabilités;
- utiliser les actifs informationnels aux fins pour lesquels ils sont destinés et selon les accès qui lui sont accordés;
- aviser sans délai le responsable de la sécurité de l'information de tout problème concernant la sécurité de l'information.
- se soumettre aux processus de confidentialité exigé par l'organisation.

8. APPROBATION ET DATE D'ENTRÉE EN VIGUEUR

Cette politique est en vigueur et fera l'objet d'une révision bisannuelle ou immédiatement en cas de changement majeur.

Vicky Poirier, CPA, CA, CA·EJC, CFF
Présidente, Quantum Juricomptable inc. et ALIAS^{MC}