| CHAMBRE DE L'ASSURANCE DE DOMMAGES | POLITIQUE | |
|---|---|---|
| | DATE DE LA RÉSOLUTION ET DE L'ENTRÉE EN VIGUEUR :<br>**2014-12-09** | HISTORIQUE ET DERNIÈRE MISE À JOUR :<br>**2017-09-12** |
| | APPROUVÉ PAR :<br>**Conseil d'administration** | DATE D'ABROGATION :<br>**AAAA-MM-JJ** |

# Politique de gestion et de sécurité de l'information à la Chambre de l'assurance de dommages

# 1 Contexte

Afin d'assurer la protection du public, la Chambre de l'assurance de dommages (ChAD) maximise les liens de confiance entre les représentants et l'industrie de l'assurance de dommages, le public et l'Autorité des marchés financiers. La sécurité des informations traitées ou utilisées quotidiennement par la ChAD revêt une importance capitale pour l'organisation. Elle repose sur la mise en place d'une politique visant à établir les conditions générales nécessaires pour préserver la confidentialité, garantir l'intégrité et assurer la disponibilité de l'information.

Par conséquent, l'application de la politique de gestion et de sécurité de l'information touche non seulement la ChAD et ses employés, mais aussi les membres de comité, les fournisseurs et partenaires.

## 1.1 Objectifs

La ChAD traite et communique de l'information sous plusieurs formes. Cette information peut avoir une valeur légale, administrative ou économique, et est essentielle à la poursuite des activités de la ChAD. L'objectif de la présente politique est d'une part d'atténuer les risques auxquels peuvent être exposés les actifs informationnels de l'organisation, et d'assurer aussi que les mesures de protection adéquates soient déployées. Ces mesures visent principalement à minimiser les risques d'atteinte à la vie privée, de tentative d'attaque ou de vol de données en assurant :

- **la confidentialité** : le caractère réservé d'une information dont l'accès et la diffusion sont limités aux seules personnes autorisées à la connaître ;
- **l'intégrité** : la protection de l'exactitude et de l'entièreté de l'information et des méthodes de traitement de celle-ci ;
- **la disponibilité** : la capacité d'assurer l'accès à l'information et aux méthodes de traitement de celle-ci de manière ininterrompue, sans délai ou dégradation, au moment où la sollicitation en est faite, et la capacité d'assurer la pérennité de l'information.

# 2 Application

## 2.1 Personnes visées

Cette politique s'applique à toutes les personnes physiques ou morales ayant accès, sur place ou à distance, aux actifs informationnels, aux biens ou aux lieux pour lesquels la ChAD est responsable d'assurer la sécurité.

Sauf indication contraire, la politique s'applique à tous les individus qui se voient accorder l'accès aux actifs informationnels de la ChAD, qu'il s'agisse d'un gestionnaire, d'un administrateur, d'un employé, d'un partenaire, d'un fournisseur ou d'un mandataire agissant légalement au nom de la ChAD.

### 2.2 Informations visées

Cette politique s'applique sans exception à tout actif informationnel sous la responsabilité de la ChAD, et ce, quel que soit son support. Toute activité visant la manipulation ou l'utilisation d'information est par conséquent assujettie à la présente politique, tout au long de son cycle de vie.

## 3 Principes directeurs

La ChAD s'engage à assurer la sécurité de ses actifs informationnels quels qu'ils soient, conformément aux principes directeurs suivants.

### 3.1 Gestion du risque

Le choix des mesures de sécurité des actifs informationnels s'appuient sur l'identification et l'évaluation périodique des risques qui en menacent la confidentialité, l'intégrité ou la disponibilité. Ainsi, les mesures de protection seront déployées en fonction de l'évaluation des impacts et de la probabilité d'occurrence d'une menace, afin d'en atténuer les risques et de les maintenir à un niveau acceptable en fonction des obligations de l'organisation.

Tout changement important aux systèmes de traitement des actifs informationnels doit en outre faire l'objet d'une analyse de risque détaillée avant sa mise en place.

### 3.2 Formation et sensibilisation

L'aspect humain est un des éléments fondamentaux de la protection de l'information. Il importe donc de sensibiliser les personnes visées aux menaces et aux conséquences d'une atteinte à la sécurité pour que chacun puisse développer les réflexes nécessaires pour reconnaître les risques potentiels et y pallier de manière efficace afin d'assurer la sécurité des actifs informationnels de l'organisation. La formation et la sensibilisation à la sécurité informationnelle sont essentielles pour assurer la protection adéquate de l'information.

Tout employé est en droit de recevoir les renseignements nécessaires à la bonne compréhension de ses responsabilités en matière de sécurité informationnelle. L'employé aura notamment accès à la *Directive encadrant l'utilisation des technologies de l'information* et la *Politique de sécurité des renseignements personnels et confidentiels de la ChAD* ainsi qu'à d'autres documents, communications et séances de formation.

Les employés peuvent en tout temps se référer au Directeur des services administratifs pour obtenir des explications ou des renseignements supplémentaires quant aux modalités d'utilisation et de protection des actifs informationnels, ou pour signaler tout incident ou menace susceptible de compromettre la sécurité des actifs informationnels de l'organisation.

## 3.3 Gestion et exploitation des systèmes

Les services administratifs assurent la gestion et l’exploitation de l’ensemble des systèmes informationnels de la ChAD en déployant entre autres les mesures appropriées pour minimiser le risque de panne des systèmes, et assurer le fonctionnement optimal de ceux-ci. Certains de ces mécanismes effectuent la surveillance complète des systèmes afin d’en détecter les défaillances et de contrer tout traitement non-autorisé ou malveillant.

Les services administratifs assurent aussi la protection et la sécurité physique tant de ses employés que de ses ressources informationnelles. De plus, la sécurité logique est partie intégrante de la protection des actifs informationnels de la ChAD, et l’accès à ces actifs est strictement contrôlé par les services administratifs en fonction des besoins de chaque employé.

## 3.4 Responsabilité des intervenants

La protection des actifs informationnels de la ChAD repose aussi sur l'engagement continu de l'ensemble des intervenants. Chacun a l'obligation de protéger l'information et le matériel mis à sa disposition. Les intervenants ont des responsabilités spécifiques en matière de sécurité et sont redevables de leurs actions.

## 3.5 Relève et continuité

La ChAD doit assurer la continuité des activités nécessaires à la réalisation de sa mission en cas de sinistre ou de défaillance majeure ayant un impact sur les actifs informationnels jugés essentiels. Le plan de continuité de la ChAD a été élaboré afin de minimiser les impacts d’un sinistre ou d’une défaillance majeure de ses systèmes et d’assurer la poursuite des activités et des services essentiels.

# 4 Entrée en vigueur et révision

La présente politique entre en vigueur dès son adoption par le conseil d’administration de la ChAD.