BARSALOU
LAWSON
RHEAULT

PL01 - Politique de sécurité de l'information

Politique – Sécurité de l'information

Table des matières

Politique – Sécurité de l'information

1. PRÉAMBULE

Afin de mener à bien ses activités, *Barsalou Lawson Rheault* (ci-après " BLR ") génère, stocke, traite et communique des informations sous de nombreuses formes. Elle reconnaît que ces actifs informationnels, essentiels à son activité, doivent être évalués, utilisés de manière appropriée et protégés de manière adéquate tout au long de leur cycle de vie. A cette fin, il est nécessaire de mettre en œuvre un ensemble cohérent de mesures de sécurité déterminées par une approche de gestion des risques de sécurité basée sur les meilleures pratiques, en conformité avec les exigences législatives et réglementaires.

Les actifs informationnels couverts par la présente politique de sécurité des actifs informationnels comprennent non seulement les informations, mais aussi les équipements et les supports (papier ou numérique). Ils comprennent les données, les documents, les liens de communication internes, les sites d'hébergement, les ordinateurs (IT), les appareils mobiles et autres équipements portables. La politique représente un objectif à atteindre par la BLR dans les trois ans suivant son adoption.

2. Introduction

2.1. DÉFINITIONS

Les définitions des différents termes utilisés dans cette politique et dans d'autres documents associés sont disponibles dans le glossaire de la sécurité de l'information.

2.2. OBJECTIFS

Le présent document constitue la *Politique de sécurité des actifs informationnels de* la BLR (ci-après la "Politique") qui établit les pratiques à adopter pour se conformer à diverses obligations légales et administratives et pour protéger tous les actifs informationnels et prévenir les incidents de sécurité potentiels, y compris la fraude, les fuites d'informations, les attaques informatiques, les erreurs accidentelles, les actions délibérées et l'atteinte à la vie privée. De cette manière, la BLR protège ses actifs et atténue les risques liés à la confidentialité, à l'intégrité et à la disponibilité des informations.

2.3. CHAMP D'APPLICATION

La présente politique s'applique à tout actif informationnel détenu par la BLR et les sociétés associées, y compris les informations collectées dans le cadre d'activités contractuelles, réglementaires et légales.

Sans limiter la portée de ce qui précède, aux fins de la présente politique, les personnes suivantes seront considérées comme des parties prenantes de BLR, son personnel, ses administrateurs, ses sous-traitants, ses fournisseurs, ses partenaires et ses agents.

2.4. ENGAGEMENT DU COMITÉ DE GESTION

Cette politique s'inscrit dans une démarche globale de prévention et de sensibilisation à la sécurité de l'information. Pour ce faire, la collaboration de toutes les parties prenantes est essentielle. Le comité de gestion s'engage à prendre tous les moyens nécessaires pour soutenir les actions à entreprendre dans la mise en œuvre de cette politique, ainsi que dans la mise en œuvre des cadres associés.

2.5. PROPRIÉTAIRE DE POLITIQUE ET DU CADRE DE SÉCURITÉ DE L'INFORMATION

La présente politique et les divers cadres de sécurité associés relèvent du responsable de la sécurité de l'information (RSI). Le RSSI doit en assurer la maintenance, la révision et la communication.

2.6. SUIVI ET CONTRÔLE DES ACTIVITÉS DE SÉCURITÉ DE L'INFORMATION

Afin de surveiller son exposition aux risques, la BLR doit disposer d'une infrastructure de surveillance et de processus de soutien. Elle doit permettre de contrôler en permanence l'efficacité de ses méthodes, processus et mécanismes de protection et de les améliorer en fonction de l'évolution des risques auxquels la BLR est confrontée.

BLR se réserve le droit, sans préavis, de surveiller tout actif informationnel et toute information détenue, traitée et exécutée sur ses systèmes et appareils mobiles. Ce privilège doit toujours être exercé conformément aux lois et lorsque des motifs raisonnables le recommandent.

2.7. CONSÉQUENCES

Le non-respect de la présente politique ou des cadres de sécurité associés peut amener BLR à retirer les droits d'accès à un employé et à appliquer des mesures disciplinaires ou juridiques. Toute partie prenante ayant connaissance du non-respect ou de l'omission de la présente politique doit en informer le RSI ou un membre du comité de gestion.

2.8. RESPECT DE LA POLITIQUE

Les requis de sécurité doivent être appliqués à l'appui des besoins commerciaux de BLR et ne doivent en aucun cas devenir une contrainte sans valeur ajoutée ou qui empêche la BLR d'offrir ses services à ses clients.

Compte tenu de ce qui précède, il est possible que, dans le cadre des opérations normales, des situations spécifiques rendent impossible le respect de certaines exigences en matière de sécurité de l'information. Dans un tel contexte, une procédure claire de gestion de la non-conformité aux exigences de sécurité est nécessaire pour garantir qu'elles sont correctement analysées, approuvées et suivies.

3. Principes généraux

3.1. ORGANISATION INTERNE

Afin d'assurer une gestion efficace de la sécurité de l'information au sein de BLR, il est important de définir la structure organisationnelle de BLR qui soutient la planification, le développement, la mise en œuvre et le contrôle des mesures de sécurité. Le comité de gestion est chargé de veiller à ce que la structure de sécurité de l'information de la BLR soit définie et mise en œuvre.

3.2. ÉVALUATION ET GESTION DES RISQUES LIÉS AUX ACTIFS INFORMATIONNELS

Les mesures de sécurité mises en place sont basées sur l'évaluation, l'analyse périodique et le traitement par BLR des risques relatifs à la confidentialité, à l'intégrité et à la disponibilité des informations.

Une évaluation des risques doit être effectuée avant de procéder à l'acquisition de nouveaux systèmes ou d'effectuer un changement susceptible d'avoir un impact sur la sécurité des actifs informationnels de BLR. Dans tous les cas, cette évaluation doit être documentée en suivant un processus défini.

3.3. SÉCURITÉ DES RESSOURCES HUMAINES

BLR met en place des processus de sécurité des ressources humaines dans le but de réduire le risque d'erreur humaine, de vol, de fraude ou d'utilisation abusive des actifs informationnels de BLR avant l'embauche, pendant la période d'emploi et après le départ de l'employé.

3.4. GESTION DU PATRIMOINE INFORMATIONNEL

Afin de mettre en place et de maintenir une protection appropriée, chaque actif informationnel doit être inventorié et se voir attribuer un propriétaire qui connaît sa valeur et son importance pour l'organisation. Le propriétaire établira sa classification en fonction de sa valeur et de son importance pour l'organisation afin d'établir un niveau de protection approprié.

3.5. CONTRÔLE D'ACCÈS AUX ACTIFS INFORMATIONNELS

3.5.1. "PRINCIPE DU "BESOIN DE SAVOIR

Les informations ne doivent être divulguées qu'aux personnes qui en ont besoin dans le cadre de leurs fonctions et conformément aux obligations législatives et réglementaires.

3.5.2. GESTION DE L'ACCÈS

La gestion de l'accès doit être effectuée selon des processus et des procédures formels, convenus et communiqués aux personnes concernées.

Lorsqu'un utilisateur change d'emploi (licenciement, transfert, promotion ou congé de longue durée), son gestionnaire doit revoir ses accès.

Les propriétaires, en collaboration avec le RSSI, doivent s'assurer qu'un examen périodique des comptes d'utilisateurs est effectué.

3.5.3. CONTRÔLES D'ACCÈS

Tout actif informationnel qui conserve des informations non classées comme publiques doit disposer d'un mécanisme d'authentification actif pour garantir que ces informations ne sont pas indûment divulguées, modifiées, supprimées ou rendues indisponibles.

Les utilisateurs doivent disposer d'un identifiant unique et ne doivent en aucun cas le partager.

3.6. SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

Tous les actifs informationnels doivent être protégés par des mesures de sécurité physique en fonction de leur niveau de sécurité, des risques associés et de leur valeur pour BLR.

L'accès aux bureaux et aux salles informatiques contenant des informations non classées comme publiques doit être physiquement limité par un mécanisme de sécurité approprié.

3.7. GESTION DES OPÉRATIONS INFORMATIQUES ET TÉLÉCOMMUNICATIONS

À moins qu'elle n'ait été désignée comme "publique", toute information doit être protégée contre toute divulgation non autorisée à des tiers. Les tiers ne peuvent avoir accès aux informations non classées comme publiques que si un besoin a été démontré et que la divulgation a été autorisée par le propriétaire ou par la loi.

3.8. ACQUISITION, DÉVELOPPEMENT ET MISE À JOUR DES SYSTÈMES

Les exigences de sécurité à respecter lors de l'acquisition, du développement, de la mise en œuvre et de la maintenance d'un bien d'information doivent être déterminées. Les exigences de sécurité doivent tenir compte des évolutions technologiques et des nouveaux défis en matière de sécurité.

3.9. GESTION DES INCIDENTS

BLR doit établir et définir les responsabilités et les procédures à mettre en œuvre en cas d'incident de sécurité afin de garantir une réponse efficace et pertinente tout en assurant la mise en place d'une équipe capable de gérer les incidents.

3.10. REPRISE APRÈS SINISTRE

La BLR doit mettre en œuvre un plan de reprise des technologies de l'information ("*Disaster recovery plan*") visant à réduire l'impact de l'indisponibilité d'un actif informationnel et à assurer ainsi une reprise informatique dans les plus brefs délais. Les mesures de récupération doivent être vérifiées périodiquement pour s'assurer qu'elles sont efficaces et pertinentes.

3.11. FORMATION ET SENSIBILISATION

BLR doit sensibiliser les employés aux menaces et aux conséquences d'une violation de la sécurité afin que chacun puisse reconnaître les situations à risque et agir en conséquence.

Un programme de formation et de sensibilisation à la sécurité de l'information adapté aux différents rôles des employés doit être défini.

Il incombe à BLR de fournir à toute personne devant accéder aux actifs informationnels les lignes directrices nécessaires pour comprendre ses responsabilités en matière de sécurité de l'information.

Tous les documents pertinents doivent être communiqués aux employés, y compris la présente politique et les cadres associés.

4. Rôles et responsabilités

4.1. COMITÉ DE GESTION

Le comité de gestion de la BLR est chargé de veiller à ce que des cadres de sécurité adéquats soient élaborés et maintenus au sein de l'organisation. Le comité est chargé d'approuver la présente politique et de prendre tous les moyens nécessaires pour la mettre en œuvre, ainsi que les autres documents associés.

4.2. RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (CISO)

Le RSI est le représentant principal de la BLR pour toutes les questions relatives à la sécurité des actifs informationnels. Sans limiter la généralité de ce qui précède, le RSI doit notamment

- Rendre compte chaque année au comité de gestion du respect de la politique et soumettre un rapport de conformité.
- Maintenir la politique à jour en fonction des besoins, des obligations et des préoccupations de BLR. Veiller à ce que les différentes parties prenantes participent à l'élaboration de cette politique et d'autres cadres associés.
- Définir les critères de sécurité pour les technologies utilisées au sein de BLR.
- Fournir des conseils en matière de sécurité de l'information.
- Procéder à des évaluations des risques et des vulnérabilités dans tous les projets impliquant un actif informationnel, ce qui permet de définir les besoins de sécurité pour assurer la protection des actifs informationnels.
- Sensibiliser tous les utilisateurs à la sécurité de l'information.
- Assurer une gestion efficace des incidents de sécurité et la maintenance du plan de reprise après sinistre (DRP) sur la base du plan de continuité des activités (BCP).

4.3. PROPRIÉTAIRE DU PATRIMOINE INFORMATIONNEL

Le propriétaire d'un actif informationnel est le responsable d'un secteur d'activité de BLR. Il est responsable, du point de vue de l'entreprise, des actifs informationnels nécessaires à la conduite des activités de son département, tels que :

- Déterminer la valeur de ses actifs informationnels pour sa gestion et assurer leur classification conformément à celle-ci.
- Identifier et assurer la mise en œuvre des mesures et des contrôles de sécurité afin de garantir la protection des actifs informationnels conformément au niveau de sécurité attribué et aux évaluations des risques.
- Assurer le maintien des mesures de sécurité pour tous ses actifs tout au long de leur cycle de vie (création, maintenance, conservation, destruction, etc.)
- Approuver l'attribution des droits d'accès aux actifs informationnels sous sa responsabilité en fonction des besoins requis.
- Veiller à ce qu'un plan de reprise après sinistre, spécifique à ses actifs informationnels, soit en place et testé régulièrement.

4.4. UTILISATEUR D'ACTIFS D'INFORMATION

L'utilisateur d'un actif informationnel est une personne à qui un propriétaire a accordé l'accès à un ou plusieurs actifs informationnels de BLR. Un utilisateur peut être permanent, temporaire, administrateur, contractant, consultant ou un tiers.

Lorsque la valeur du bien informationnel le justifie, des accords spéciaux avec un tiers (tels que des accords de confidentialité) doivent avoir été conclus avant l'attribution du contrat ou la cession.

Son rôle consiste, entre autres, à mener à bien les tâches suivantes :

- N'utiliser les actifs informationnels qu'à des fins expressément approuvées par le propriétaire.
- Respecter toutes les mesures de sécurité en place.
- S'abstenir de divulguer les informations en leur possession (sauf si elles ont été désignées comme publiques) sans l'autorisation préalable de leur propriétaire.
- Informer le responsable de la sécurité de l'information de toutes les situations dans lesquelles il estime que la sécurité d'un actif informationnel est vulnérable ou a été compromise.
- se conformer à la présente politique et à tout autre document qui s'y réfère ou la soutient.

5. EXAMEN ET APPROBATION

La présente politique entre en vigueur dès son adoption par le comité de gestion et peut être révisée à tout moment par le responsable de la sécurité de l'information (RSI).

Des modifications peuvent être proposées par diverses parties prenantes de BLR, qui doivent être soumises par écrit au responsable de la sécurité de l'information (RSI).

La présente politique doit être réexaminée au moins tous les deux ans afin de s'assurer de sa pertinence par rapport à la mission de BLR, aux activités de ses utilisateurs et à toute modification substantielle de la législation ou des exigences réglementaires.

6. DATE D'ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le 1er août 2023. Elle remplace toutes les lignes directrices antérieures sur ce sujet.