PUIG

Politique de sécurité des informations

Contexte

Le Code d'éthique de **Puig** établit que les actifs de données et d'information sont des actifs dont la collecte et le traitement doivent être limités à ce qui est strictement nécessaire à l'exercice des activités légitimes de l'entreprise, et promeut un cadre proactif pour leur protection.

Objectif et champ d'application

La présente Politique détaille les engagements établis dans le Code d'éthique de **Puig** et définit les principes et les mesures qui constituent le cadre du traitement, de la gestion et de la sécurité des données ou des actifs informationnels. Les données ou actifs informationnels sont tout type de ressource qui contient des informations nécessaires à l'activité de l'entreprise, indépendamment de la plateforme, du canal ou de la manière dont elles sont communiquées, transmises, partagées, projetées ou stockées, qu'elles soient internes ou externes, ou qu'elles soient détenues par **Puig** ou par des tiers.

L'objectif de cette politique est de fournir à **Puig** un cadre pour la protection des données et des actifs informationnels afin de préserver leur confidentialité, leur intégrité et leur disponibilité, et de veiller à la conformité aux réglementations en vigueur relatives à la sécurité des informations.

La présente Politique a été approuvée par le Conseil d'administration de **Puig** Brands, S.A. et s'applique à toutes les sociétés et activités[1] de **Puig**.

La présente Politique est le cadre générique qui définit les principes et les mesures à mettre en œuvre par les personnes responsables des actifs de données et informationnels dans chaque domaine fonctionnel.

Des divisions et unités opérationnelles spécifiques de **Puig** peuvent élaborer la présente Politique par le biais d'autres réglementations divisionnaires ou locales qui sont conformes aux dispositions de la présente Politique.

[1] « **Puig** » désigne la société **Puig** Brands, S.A. et ses filiales et autres entités qui peuvent être constituées à l'avenir et dans lesquelles **Puig** Brands, S.A. détient ou peut détenir un contrôle direct ou indirect, conformément à l'article 42 du Code de commerce espagnol.

Principes et mesures découlant de la présente Politique

Principes

La présente Politique est fondée sur les principes suivants :

- **Protection de l'activité**, en donnant la priorité à la protection des informations qui affectent directement les opérations commerciales, l'innovation et l'amélioration continue de nos activités.

- **Gestion des risques**, adoption de mesures pour identifier les risques existants dans la gestion des informations et éviter ceux qui sont inutiles ou excessifs.

Mesures

Pour se conformer aux objectifs et principes établis, les mesures suivantes sont nécessaires :

- **Classification des informations** : Tous les actifs informationnels doivent être identifiés et classés en termes de valeur, d'exigences légales, de confidentialité, de sensibilité et d'importance pour l'entreprise. Les propriétaires des actifs sont chargés de s'assurer qu'ils sont correctement classés et protégés selon la classification suivante en tenant compte de la loi et des bonnes pratiques, de leur impact potentiel sur l'entreprise et son image, et sur les partenaires ou autres entités liées à **Puig** :

    - Informations secrètes : informations d'importance stratégique pouvant avoir un impact grave ou irréparable et dont l'accès est limité à un très petit groupe de personnes.

    - Informations restreintes : informations sensibles appartenant à un secteur d'activité ou à un département qui peuvent donner lieu à des pertes économiques modérées, à des violations des réglementations en vigueur ou à une atteinte à la réputation de **Puig**, entre autres conséquences potentielles. Elles ne sont accessibles qu'à un groupe spécifique de personnes expressément autorisées par le propriétaire des informations.

- Informations confidentielles : informations pouvant avoir un impact grave et dont l'accès est limité à un groupe spécifique de personnes, à des zones spécifiques ou à des zones partielles.

- Informations internes : informations qui peuvent avoir un impact limité et qui sont généralement accessibles à l'ensemble ou à la plupart des personnes, bien qu'elles ne puissent pas être divulguées publiquement.

- Informations publiques : informations qui sont dans le domaine public ou qui sont mises à la disposition du public par le biais d'un canal **Puig** et qui peuvent être librement consultées.

- **Gestion de la sécurité des informations** : un niveau adéquat de protection, de contrôle et de gestion des actifs informationnels de **Puig** est garanti.

- **Gestion des incidents** : des procédures sont établies pour la gestion des incidents de sécurité des informations qui comprennent la notification, la réponse et la récupération.

- **Contrôle d'identité** : le cycle de vie des identités et les comptes associés à chacune d'elles doivent être contrôlés et gérés de manière appropriée.

- **Contrôle d'accès** : l'accès aux informations doit être contrôlé et limité aux personnes autorisées, et les droits d'accès doivent être examinés régulièrement pour s'assurer qu'ils sont adéquats.

- **Continuité de l'activité** : en cas d'interruptions ou de défaillances éventuelles des opérations commerciales, des plans sont élaborés à l'avance pour garantir sa continuité, tout en protégeant, en maintenant et en récupérant les informations.

- **Formation et sensibilisation** : des initiatives de formation et de sensibilisation sont mises en œuvre pour garantir la sécurité des informations pour les utilisateurs.

- **Conformité** : la conformité aux réglementations en vigueur en matière de sécurité des informations est garantie.

- **Examen et amélioration continue** : Des activités d'audits et d'examen régulières seront menées pour évaluer l'efficacité de la Politique de sécurité des informations et des pratiques de sécurité des informations.

Puig garantit les principes, les mesures et la méthodologie inclus dans la présente Politique en fournissant les ressources matérielles, technologiques, financières et humaines nécessaires.

Application et responsabilités

La présente Politique est obligatoire pour toute personne ou entité juridique ayant accès aux données ou aux actifs informationnels de **Puig**, et toutes les parties intéressées doivent promouvoir la conformité à la présente Politique.

Le non-respect de la présente Politique peut entraîner des mesures disciplinaires et d'autres conséquences prévues par la loi.

Approbation, publication et examen

La présente Politique a été approuvée par le Conseil d'administration de **Puig** Brands, S.A. le 5 avril 2024, et est entrée en vigueur à cette date.

La responsabilité de la publication, de la communication et de l'examen de la présente Politique est assignée au Domaine de la sécurité des informations et de la cybersécurité en coordination avec le Domaine juridique.