IDEUZO at_work

Le Manifeste IT responsable

Mise à jour le 17/04/2023

Tableau de révision de la procédure interne

Version	Date de modification	Rédacteur	Eléments modifiés
V1	01/09/2024	Elodie FRIOT	Création du document

PREAMBULE

CCe manifeste IT formalise les engagements, principes directeurs et pratiques de gestion des systèmes d'information de notre agence de communication et Marketing RH IDEUZO at_work. Il vise à garantir un usage éthique, sécurisé, et efficace des technologies de l'information, en conformité avec les réglementations en vigueur, ainsi qu'avec les attentes de nos collaborateurs, clients, et fournisseurs..

Les objectifs de ce Manifeste

1- Structurer et formaliser nos engagements IT pour aligner notre organisation avec les meilleures pratiques existantes.

2- Assurer la conformité légale et réglementaire, notamment en matière de cybersécurité, de protection des données et de lutte contre la corruption.

3- Renforcer la confiance et la transparence auprès de nos parties prenantes : clients, fournisseurs, collaborateurs et partenaires.

4- Garantir l'excellence opérationnelle, en intégrant des outils et des processus efficaces qui soutiennent nos objectifs stratégiques et opérationnels.

5- Créer un cadre évolutif pour anticiper les besoins futurs et répondre aux nouveaux enjeux technologiques.

IDEUZO at_work

1 Les principes généraux

1-1 La transparence

Nous adoptons une communication proactive sur nos pratiques IT, incluant la gestion des données, la cybersécurité et les relations avec nos parties prenantes.
Une mise à jour annuelle sur l'état de nos systèmes et de nos politiques IT seront rendus accessibles aux parties concernées, dans la mesure du possible.

1-2 Ethique & Conformité

Nos systèmes IT sont conçus pour respecter les réglementations en vigueur.
Toute activité IT est soumise à un contrôle rigoureux pour prévenir les pratiques non conformes, les conflits d'intérêt et les abus potentiels.

1-3 Innovation responsable

L'adoption de nouvelles technologies est guidée par des analyses d'impact détaillées sur les utilisateurs, les données, et l'environnement.
Nous privilégions des solutions éthiques lorsque cela est possible, en réduisant notre dépendance à des acteurs monopolistiques.

2 La sécurité et la protection des données

2-1 Cybersécurité

Chaque poste de travail est équipé de solutions de sécurité actualisées, incluant pare-feu et antivirus.
Les accès aux systèmes critiques sont protégés par une politique de mots de passe robuste.
Une cellule de veille technologique surveille en permanence les menaces émergentes et adapte nos systèmes en conséquence.

2-2 La protection des données

Les données de nos clients, collaborateurs et partenaires sont stockées et protégées par notre politique de mots de passe.
Des audits réguliers de nos bases de données permettent de vérifier leur conformité avec les normes de confidentialité.
En cas de traitement de données pour des tiers, nous nous assurons que chaque partie concernée a donné son consentement explicite et informé.

2-3 Gestion des incidents

Un Plan de Continuité d'Activité (PCA) garantit le maintien des opérations essentielles en cas de cyberattaque ou de panne majeure.
En cas d'incident, un rapport détaillé sera établi et partagé avec les parties prenantes concernées, tout en respectant les obligations légales de notification aux autorités compétentes.

3 Les obligations légales & la responsabilité

3-1 La conformité avec la Loi Sapin II

Un registre informatique des transactions est maintenu pour garantir la traçabilité et l'intégrité des données financières.
Des formations sur l'éthique et la conformité sont dispensées à l'ensemble des collaborateurs utilisant nos outils IT.
Une solution de signalement interne anonyme est disponible pour toute personne souhaitant alerter sur une activité suspecte.

3-2 La responsabilité partagée

Nous imposons à nos fournisseurs IT des clauses contractuelles garantissant leur adhésion à des standards de sécurité et d'éthique équivalents aux nôtres.
Un suivi annuel des partenaires stratégiques permet de nous assurer qu'ils respectent leurs engagements.

4 La collaboration avec notre ecosystème

4-1 L'engagement envers nos clients

Un support technique dédié est disponible pour résoudre rapidement les problèmes liés aux outils technologiques et à nos prestations commercialisées.

4-2 La relation avec nos fournisseurs

Un processus d'évaluation annuel garantit que nos fournisseurs IT respectent des critères stricts de performance et de conformité, que leurs services répondent à nos attentes et évoluent en parallèle de nos besoins.

4-3 La collaboration interne

Nos collaborateurs bénéficient d'outils intuitifs, interconnectés et sécurisés, favorisant un travail collaboratif sans compromis sur la sécurité.

5 Développement durable & IT

Tous les équipements en fin de vie sont recyclés via des filières spécialisées. L'achat de matériel neuf est limité aux cas strictement nécessaires, privilégiant la réutilisation ou la réparation des équipements existants.
Des campagnes de sensibilisation à la réduction des déchets numériques (mails inutiles, stockage de fichiers non utilisés) sont organisées régulièrement.

6 Mesure et Evaluation

6-1 Notre comité éthique

Un comité de conformité éthique supervise et coordonne les efforts en matière de pratiques éthiques et responsables. Il assure la communication interne sur les questions éthiques et protection des données et gère les enquêtes internes.

Olivier LETORT
PDG

Ivan ORGEBIN
DGA

Vincent BOMAL
DAF

Elodie FRIOT
Resp. RSE

Jonathan BUFFET
Directeur Commercial

Mélanie GUERRA
RRH

6-2 Assurance Cyber Sécurité

IDEUZO a souscrit une assurance CYBER SECURITE garantissant les conséquences financières des risques immatériels pouvant affecter les systèmes informatiques, et les données personnelles des clients et des collaborateurs de l'entreprise assurée.

Couvertures et engagements

L'assurance cyber Stoïk nous permet de renforcer notre stratégie de gestion des risques informatiques grâce aux garanties suivantes :

- Plafond global : Une couverture jusqu'à 1 000 000 € par période d'assurance.
- Franchise : 5 000 € par sinistre, avec une réduction de 25 % si l'ensemble des outils de prévention Stoïk Protect sont en place.

Garanties principales

Notre assurance cyber offre des garanties essentielles pour protéger les données personnelles et assurer la continuité de nos activités :

- Gestion de crise et remise en état du système en cas d'incident de cybersécurité.
- Frais de notification et surveillance suite à une fuite de données, conformément aux obligations du RGPD.
- Indemnisation des pertes d'exploitation jusqu'à 6 mois (délai de carence de 12h).
- Protection contre la cyber-extorsion et la cyber-fraude (limitée à 10 % du montant des garanties, avec un maximum de 50 000 €).
- Responsabilité civile en cas d'atteinte aux données personnelles ou de transmission de virus.
- Couverture des sanctions administratives éventuellement imposées par la CNIL.

En plus des garanties financières, notre assurance cyber inclut un accompagnement technique préventif et réactif :

- Assistance 24/7 avec une hotline dédiée et une équipe spécialisée en gestion des incidents.
- Accès à la plateforme Stoïk Protect, comprenant :
  - Un scan hebdomadaire des vulnérabilités externes.
  - Une analyse des configurations Cloud et Active Directory.
  - Des simulations de phishing pour sensibiliser les employés.
  - Des modules de formation à la cybersécurité