Politique de cybersécurité (BAsic)

Modèle

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents** |  |
| Auteur |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date d'approbation** | **Approuvé par** | **Description du changement** |
|  |  |  |  |

# Intro

**[L'organisation]** reconnaît le rôle crucial que joue l'information dans les objectifs commerciaux d'aujourd'hui. Dans un monde moderne, les systèmes d'information doivent être fortement interconnectés et accessibles de partout. Si cette situation offre de grandes opportunités, le risque d'attaques hostiles ou de perte de données augmente rapidement.

La présente politique de cybersécurité définit les exigences minimales applicables à tous les départements de **[l'organisation]** afin deprotéger notre propriété intellectuelle, notre avantage commercial et notre personnel des conséquences d'une mauvaise sécurité de l'information et de toute cyberattaque.

Bien entendu, le respect des lois et des règlements est également pris en compte.

Le cas échéant, les services peuvent définir des lignes directrices supplémentaires et prendre des mesures additionnelles pour assurer le niveau de sécurité requis.

# Principes politiques

**Nous disposons de politiques et de procédures efficaces**

Nous sommes conscients des risques liés à la sécurité de l'information. Nous élaborons ensemble des politiques et des procédures de sécurité. Nous savons qui est responsable et comment nous appliquons les règles et les procédures.

**Nous connaissons notre environnement et gérons les risques**

Nous savons quels systèmes d'information sont importants pour **[l'Organisation].** Nous connaissons les risques liés à ces systèmes et les maintenons à des niveaux acceptables. Un cycle d'amélioration continue garantit que nos niveaux de sécurité continuent à s'adapter aux changements de notre organisation et de notre environnement.

**Nous créons des produits et/ou des services sûrs**

Les produits et services de **[l’Organisation]** sont conçus, testés et entretenus dans un souci de cybersécurité et de respect de la vie privée.

**Nous maintenons une infrastructure solide**

L'infrastructure dont dépendent les systèmes vitaux est conçue pour être hautement disponible.

**Nous agissons de manière proactive**

Nous appliquons régulièrement des correctifs. Nous comprenons les vulnérabilités de notre infrastructure et nous nous tenons au courant des vulnérabilités nouvellement découvertes. Nous tirons des enseignements des événements et des incidents liés à la sécurité.

**Nous traitons les données personnelles de manière appropriée.**

Nous collectons, utilisons et conservons les données à caractère personnel conformément à la directive AVG ((EU) 2016/679). Cela signifie que nous fournissons les mesures techniques et organisationnelles nécessaires.

# Champ d'application

D'une manière générale, la présente politique de cybersécurité s'applique à toutes les informations et à tous les systèmes de **[l'Organisation],** ainsi qu’

... aux systèmes d'information qu'ils fournissent,

... aux personnes (internes et externes) qui la traitent,

... aux appareils utilisés pour le traiter,

... aux procédures dont il dépend,

... aux lieux où nous travaillons

... aux autres aspects qui peuvent présenter un risque.

Les informations ou systèmes critiques et confidentiels sont des informations ou des systèmes qui porteront préjudice à l'organisation si leur confidentialité, leur intégrité ou leur disponibilité sont compromises.

# Exigences minimales

Notre environnement est géré de manière à contribuer à la cybersécurité.

Il s'agit notamment de ce qui suit :

* Les rôles et les responsabilités en matière de cybersécurité sont définis et communiqués aux parties prenantes internes et externes.
* Un inventaire est établi et tenu à jour avec tous les dispositifs physiques, systèmes et logiciels utilisés au sein de l'organisation.
* Les équipements essentiels aux systèmes critiques doivent être correctement entretenus pour garantir leur disponibilité et leur intégrité. Des contrats de maintenance ou des pièces de rechange doivent être envisagés.
* Des programmes antivirus, anti-espions ou autres programmes malveillants approuvés par l'organisation doivent être installés et mis à jour sur les systèmes et les points d'extrémité identifiés par l'organisation.
* Le réseau de l'entreprise sera sécurisé conformément aux exigences définies dans la politique de sécurité du réseau.
* Les systèmes d'exploitation des clients et des serveurs ainsi que les applications recevront les correctifs et les mises à jour de sécurité nécessaires, conformément à la politique de gestion des vulnérabilités et des correctifs.
* Nos employés et sous-traitants sont régulièrement sensibilisés aux risques en matière de cybersécurité et menaces auxquels ils peuvent être confrontés et à la manière de réagir en cas d'activité suspecte. Les **10 règles d'or de la cybersécurité** sont communiquées et chaque employé ou sous-traitant doit s'engager à les respecter.
* Une bonne gestion de l'accès est mise en place en tenant compte des éléments suivants
  + Authentification multifactorielle.
  + Accès minimum. Les politiques détaillées sont décrites dans la politique d'accès.
  + Mots de passe suffisamment forts La politique détaillée est décrite dans la politique relative aux mots de passe.
  + Les systèmes critiques et confidentiels doivent au moins réussir à se connecter et à se déconnecter.
* Il doit exister une procédure de récupération des systèmes critiques en cas de sinistre. Une procédure doit être mise en place pour restaurer les documents ou enregistrements critiques s'ils sont accidentellement supprimés. Les politiques détaillées sont décrites dans le document "Politique de sauvegarde et de récupération".
* Un plan d'intervention doit être mis en place dans le cadre des incidents cybernétiques.

Le présent document d'orientation fait partie d'un ensemble de documents d'orientation destinés à aider **[l'organisation]** à mettre en place une stratégie solide en matière de cybersécurité.