Revisium

Guide de rédaction

DES POLITIQUES DE SÉCURITÉ EN COLLECTIVITÉ

www.revisium.fr

Les éléments essentiels

Sommaire

01 Introduction p3

02 Les objectifs de la politique p4

03 La gouvernance de la cybersécurité p5

04 Les différentes gestions p6

05 Sécurisations p7

06 Formations et sensibilisation p8

07 Conformité et RGPD p9

08 Contact p10

Introduction

Bienvenue dans ce guide destiné aux collectivités qui ont le souhait de prendre en main leur conformité !

Nous sommes ravis de vous accompagner dans cette démarche de protection des données des administrés.

Pourquoi se préoccuper de la sécurité des données ?

La présente politique de sécurité a pour objectif de définir les principes de sécurité applicables aux systèmes d'informations de la collectivité afin de garantir la confidentialité, l'intégrité, la disponibilité des données et des services numériques. Elle vise à protéger les systèmes d'information contre les risques et menaces liés à la cybersécurité.

Les objectifs de la politique de sécurité

Protection

Cohérence

Solutions

Une politique de sécurité est une ligne de conduite qu'il faut établir en concertation avec tous les acteurs. Elle ne doit pas contraindre sans justification logique et cohérente pour la protection des données. Le DPO est un créateur de valeur qui apporte des solutions à chaque projet incluant la protection des données.

Quelques objectifs ...

- Garantir la sécurité des systèmes d'information et des données numériques
- Protéger la confidentialité des données personnelles et sensibles traitées par la collectivité
- Assurer la disponibilité des services numériques essentiels au fonctionnement des activités
- Promouvoir la cybersécurité en intégrant des pratiques de prévention et de gestion des risques.
- Conformité avec les législations et réglementations en vigueur (notamment le RGPD).

La gouvernance de la sécurité des données

RSI : responsable de la sécurité

La personne en charge de la sécurité des systèmes d'information au sein de la collectivité ou de l'entreprise est responsable de la mise en œuvre de cette politique et de son suivi.

Comité de sécurité

Un comité composé de responsables métiers et de responsables informatiques se réunit régulièrement pour évaluer l'état de la sécurité et mettre à jour la politique.

Pourquoi est-ce indispensable aujourd'hui ?

La gouvernance des données est un enjeu primordial pour chaque collectivité, car elle protège l'intégrité et la confidentialité des informations sensibles des citoyens. Face à des cyberattaques de plus en plus fréquentes, il est vital que les élus prennent des mesures actives pour garantir cette sécurité. Désigner un Délégué à la Protection des Données (DPO) est une étape obligatoire, mais aussi stratégique : en intégrant un expert en conformité RGPD, la collectivité se protège contre les risques juridiques et technologiques. Un DPO veille non seulement au respect des règlementations, mais aussi à l'anticipation des menaces et à la mise en place d'une sécurité efficace pour contrer les cyberattaques. Protéger les données, c'est protéger la confiance des citoyens et garantir la continuité des services publics en toute sérénité.

Les gestions de la sécurité des données

Gestion des accès

L'accès aux systèmes et données est attribué en fonction des besoins de chaque utilisateur. Chaque employé doit avoir un identifiant unique et un mot de passe fort.

Gestion des identités et des droits

Les droits d'accès sont limités au strict nécessaire pour accomplir les missions professionnelles. Un contrôle périodique des droits d'accès est effectué pour assurer qu'ils sont toujours pertinents.

Gestion des incidents

Un plan de réponse aux incidents doit être établi et communiqué à tous les collaborateurs. En cas d'incident, une équipe dédiée doit être formée pour contenir l'incident et en limiter l'impact.

Authentification à deux facteurs

La MFA doit être activée pour l'accès à toute application sensible ou critique.

Zoom sur la gestion des incidents

- La gestion des incidents passe obligatoirement par un plan de réponse adapté dans lequel chaque acteur joue son rôle.
- Tous les utilisateurs doivent signaler immédiatement tout incident de sécurité ou comportement suspect à l'équipe de sécurité informatique.
- Après chaque incident, un rapport détaillé doit être rédigé pour analyser l'origine, l'impact et les mesures correctives à mettre en place.

Sécurisation des données de la collectivité

Systèmes & réseaux

Données personnelles

Données sensibles

Les données des administrés sont précieuses et méritent toute l'attention des élus et des experts. Cela inclut la sécurisation des systèmes et des réseaux utilisés grâce à des outils adaptés, la protection des données personnelles mais également des données sensibles...

Quelques éléments...

- Mises à jour régulières pour combler les failles de sécurité
- Pare-feu et antivirus configurés pour bloquer les connexions non-autorisées
- Cryptage des données sensibles stockées ou transmises
- Surveillance continue pour détecter les activités suspectes
- Protection des données personnelles (RGPD)
- Conservation des données (durée, traitement, suppression)
- Droits des personnes (gestion des demandes)
- Sécurisation des équipements mobiles
- Sécurisation du télétravail (connexion VPN)

La formation et la sensibilisation des équipes

Formation continue

Tous les élus et agents doivent suivre une formation à la cybersécurité, notamment sur les risques liés au phishing, aux ransomwares et aux bonnes pratiques en matière de sécurité des mots de passe

Simulations et tests

Des tests réguliers, tels que des simulations de phishing, doivent être réalisés pour évaluer la vigilance des collaborateurs.

Sensibiliser c'est rendre plus fort !

On dit souvent que la faille est humaine. Toutefois, il est judicieux de transformer cette faille en une force pour la collectivité. Plus vous prenez du temps pour former et sensibiliser les élus, les agents, les intervenants, les fournisseurs et les sous-traitants, plus vous renforcez la barrière de protection.
Les ateliers, les formations, les sessions exceptionnelles sont autant d'armes à votre disposition pour combattre les cybercriminels.
Le DPO dispose également d'un rôle de diffuseur des bonnes pratiques et est chargé de former et sensibiliser les collaborateurs de tous bords à la cybersécurité dans un esprit collaboratif, ludique et accessible à tous.

La conformité et les audits de sécurité

Confirmité avec la législation

La collectivité ou l'entreprise s'engage à respecter toutes les lois et réglementations en matière de protection des données personnelles, de sécurité informatique et de cybersécurité.

Les audits de sécurité

Des audits de sécurité réguliers doivent être effectués pour vérifier la conformité de la collectivité ou de l'entreprise avec cette politique et les exigences légales.

La conformité, loin d'être une contrainte !

La mise en conformité d'une collectivité avec la réglementation RGPD va bien au-delà d'une simple obligation légale : elle renforce la transparence et la confiance des citoyens. En protégeant efficacement les données personnelles, la collectivité s'engage à respecter les droits des administrés tout en sécurisant ses propres systèmes. Cette démarche proactive permet d'éviter des sanctions coûteuses et de limiter l'impact d'éventuelles cyberattaques. Désigner un Délégué à la Protection des Données (DPO) garantit un suivi continu de la conformité et des meilleures pratiques de sécurité. Ce choix est un atout pour la collectivité, car un DPO assure la protection des données et optimise les processus internes, permettant ainsi aux équipes de se concentrer sur leur mission principale : servir les citoyens.

Nous contacter !

Nous restons à votre disposition pour toute question concernant la protection des données, la cybersécurité et surtout la mise en conformité des collectivités.

Vous souhaitez en savoir plus sur la protection des données et la conformité RGPD de votre collectivité ? N'hésitez pas à nous contacter !

Ensemble, nous évaluerons vos besoins et mettrons en place des solutions adaptées pour garantir la sécurité des informations de vos citoyens. Mon expertise en tant que Délégué à la Protection des Données est à votre service pour vous accompagner dans une démarche de conformité sereine et efficace. Un simple message suffit pour initier cette collaboration. Protégez votre collectivité dès aujourd'hui !

Toute l'équipe Revisium

À bientôt !