|  |
| --- |
| **Politique d'utilisation acceptable** |
| **Organisation :** [Organisation] |
| **Classification des informations :** [Catégorie] |

Contrôle document

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Mis à jour par | Date | Description des changements |
| [Numéro de version] | [Nom, Prénom] | [Date de publication] |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Révisé par | Rôle du réviseur | Approuvé par | Date | À faire réviser par |
| [Nom, Prénom] | [Rôle] | [Nom, Prénom] | [Date de publication] | [Prochaine date de révision] |

|  |  |  |
| --- | --- | --- |
| Propriétaire du document | Une version électronique de ce document est conservée dans | Une version physique de ce document est conservée dans |
| [Nom, Prénom] | [Lieu] | [Lieu] |

Table des matières

[1. Why should you read this document? 3](#_Toc127893808)

[2. What do we expect from you? 3](#_Toc127893809)

[2.1. Accounts and passwords 3](#_Toc127893810)

[2.2. Use of the internet 3](#_Toc127893811)

[2.3. Use of equipment 3](#_Toc127893812)

[2.3.1. General rules for handling equipment 3](#_Toc127893813)

[2.3.2. Company owned devices 4](#_Toc127893814)

[2.3.3. Personally owned devices that contain company data 4](#_Toc127893815)

[2.3.4. Personal use of professional device 4](#_Toc127893816)

[2.3.5. Physical equipment 4](#_Toc127893817)

[2.4. Company and client information 4](#_Toc127893818)

[2.5. Remote working 5](#_Toc127893819)

[2.6. Unacceptable behaviour 5](#_Toc127893820)

[2.7. Monitoring and enforcement 5](#_Toc127893821)

[3. Do you have any questions? 5](#_Toc127893822)

[Annex: Implementation checklist for the acceptable use policy statements 6](#_Toc127893823)

# Pourquoi devriez-vous lire ce document ?

La sécurisation de nos ressources et de nos données relève de la responsabilité de l’ensemble des collaborateurs de [Organisation]. Cette politique d'utilisation acceptable rassemble les principales lignes de conduite à suivre par [Organisation] en matière de sécurité de l’information.

L’objectif de ce document est de décrire et d’expliquer les attentes de [Organisation] à l'égard de ses collaborateurs, la façon d’exploiter les ressources et systèmes informatiques disponibles et le comportement et les meilleures pratiques à adopter en matière de sécurité de l’information. Sur la base de cette politique, [Organisation] peut garantir la protection des données des collaborateurs, assurer la continuité des activités et réduire au mieux les risques financiers et les atteintes à sa réputation.

Cette politique s'adresse à tous les collaborateurs, les consultants et les tiers qui ont accès aux ressources, données et informations de [Organisation].

# Qu’attendons-nous de vous ?

## Comptes et mots de passe

1. Les identifiants et mots de passe des comptes de [Organisation] sont strictement personnels et confidentiels. Ne les partagez jamais et ne les divulguez à personne.
2. Choisissez toujours un mot de passe solide associant des minuscules, des majuscules, des nombres et des symboles.
3. Utilisez toujours des mots de passe différents pour les comptes personnels et professionnels.
4. Évitez d’utiliser votre messagerie électronique personnelle à des fins professionnelles et vice versa.
5. Si vous avez le moindre doute quant à la compromission de votre mot de passe, modifiez-le immédiatement et faites-en rapport à [Helpdesk IT de l’organisation].

## Utilisation d’Internet

1. Si vous avez le moindre doute quant à la véracité d'un e-mail, ne l’ouvrez pas, ne téléchargez et n'ouvrez pas la pièce jointe, et faites-en rapport à [Helpdesk IT de l’organisation] (p.ex. e-mail provenant d’expéditeurs ou de sites non identifiés).
2. Le respect de l’éthique constitue un pilier fondamental de [Organisation]. Ne vous engagez pas et ne publiez pas de contenu offensant, frauduleux, discriminatoire, obscène ou relevant du harcèlement.
3. Les informations internes et confidentielles ne sont communiquées aux destinataires que par les canaux de communication approuvés par [Organisation] et ne sont stockées que sur des sites gérés par [Organisation] avec des droits d'accès appropriés pour empêcher tout accès non autorisé.
4. N’utilisez que des plateformes de cloud approuvées par [Responsable IT] pour stocker ou échanger des documents de [Organisation].

## Utilisation de l’infrastructure

### Règles générales pour l’utilisation de l’infrastructure

1. Vous êtes responsable du matériel informatique qui vous est confié (par exemple, ordinateur portable, smartphone) et devez le protéger contre la perte, le vol et les dommages (par exemple, verrouillage).
2. Verrouillez votre appareil lorsque vous le laissez sans surveillance.
3. Ne laissez jamais un appareil, qu'il s'agisse d'un ordinateur de bureau, d'un appareil portable ou d'un support amovible, sans surveillance en dehors du bureau ou de votre domicile.
4. Soyez particulièrement vigilant à l’égard des supports amovibles, tels que les clés USB. N’utilisez que des appareils approuvés par [Organisation].
5. Si vous constatez la perte ou le vol du moindre élément de votre infrastructure ou de vos documents, signalez-le immédiatement à [Helpdesk IT de l’organisation].

### Appareils appartenant à l’entreprise

1. Modifiez le mot de passe ou le code PIN par défaut dès que vous recevez un appareil.
2. Utilisez l’authentification multifacteurs lorsque c’est possible.
3. Appliquez toujours les mises à jour de sécurité requises dès qu’elles sont disponibles.
4. Lorsque vous quittez [Organisation], rendez tout le matériel dans un bon état de propreté, assurez-vous qu'il soit complet et fonctionnel.

### Appareils personnels contenant des données de l’entreprise

1. Déclarez tous les appareils personnels que vous utilisez à des fins professionnelles à [Responsable IT] avant de les utiliser pour la première fois et familiarisez-vous avec les exigences de sécurité minimales (p. ex. installation des mises à jour, etc.).
2. [Responsable IT] déterminera le niveau d'accès au réseau pour chaque appareil personnel.
3. Les systèmes d'exploitation qui ne bénéficient plus des mises à jour de sécurité du fournisseur ne sont pas autorisés à traiter les informations de [Organisation].
4. N’utilisez que des logiciels téléchargés depuis des sources fiables (app store fiable, etc.) si vous accédez au réseau à partir d’un appareil personnel.
5. Utilisez les appareils personnels avec précaution, notamment en procédant sans attendre aux mises à jour de sécurité nécessaires et en veillant à ce qu'une solution antivirus moderne et actualisée soit installée.

### Usage privé d'appareils professionnels

1. L’infrastructure informatique vous est confiée à des fins professionnelles.
2. Un usage privé limité de l’infrastructure professionnelle est toléré à condition qu’il n’impacte pas votre travail ou la sécurité de [Organisation]. Ce droit peut être révoqué à tout moment si un abus est constaté.

### Infrastructure physique

1. Ne laissez jamais d’informations confidentielles sans surveillance.
2. Les badges d'accès sont strictement personnels. Ne les partagez jamais et ne les prêtez à personne.

## Informations sur l’entreprise et les clients

1. Les données doivent être traitées, gérées et partagées en fonction de leur niveau de confidentialité.
2. Chaque collaborateur est responsable de la sécurité des informations qui lui sont confiées.
3. Les informations relatives à [Organisation] et aux clients sont exclusivement destinées à un usage professionnel et ne peuvent être exploitées à des fins personnelles.
4. Toutes les informations acquises, générées et traitées pendant les heures de travail relèvent de la propriété intellectuelle de [Organisation].
5. Vous pouvez exclusivement copier, accéder aux et modifier les informations pour lesquelles vous disposez d'une autorisation et pouvez démontrer un besoin professionnel clair. Si des informations qui ne vous sont pas destinées sont divulguées, signalez-le à [Helpdesk IT de l’organisation].
6. Le partage d'informations ne doit se faire que par le biais de méthodes et canaux approuvés et uniquement avec les destinataires concernés.
7. Dans un lieu public, soyez toujours attentif à l'environnement lorsque vous partagez des informations. Au téléphone, ne parlez pas trop fort et isolez-vous si possible.
8. Détruisez les informations sur papier dès que vous n'en avez plus besoin.

## Travail à distance

1. Ne travaillez à distance qu’à l'aide d’appareils approuvés par [Organisation].
2. N’utilisez pas le WiFi public lorsque vous travaillez à distance.
3. Toutes les règles d’utilisation et de traitement de l’infrastructure restent applicables au travail à distance.
4. Si vous soupçonnez un incident de sécurité ou en avez la confirmation, signalez-le immédiatement à [Helpdesk IT de l’organisation].

## Comportement inacceptable

1. N’utilisez jamais les informations de [Organisation] pour obtenir un accès à un réseau ou un système non autorisé.
2. Ne modifiez ou supprimez jamais délibérément des données susceptibles d'impacter les activités professionnelles normales.
3. N’utilisez jamais de ressources de [Organisation] dans le cadre d’activités illégales ou contraires à l’éthique.
4. Ne partagez jamais de logiciels ou d'informations non autorisé(e)s ou divulgué(e)s appartenant à [Organisation].
5. Ne portez jamais délibérément atteinte aux droits de propriété intellectuelle d'autrui (p.ex. en installant des logiciels piratés, en utilisant des images protégées par un droit d'auteur trouvées en ligne, etc).
6. N’installez ou ne téléchargez jamais de logiciels contraires aux lignes de conduite de [Organisation].

## Surveillance et respect de la mise en œuvre

1. Sachez qu'afin de garantir la sécurité de ses systèmes et le respect des politiques, [Organisation] peut contrôler les activités des membres du personnel afin d'identifier les comportements intentionnels ou non intentionnels susceptibles d'avoir un impact négatif, ce qui est conforme à la politique de confidentialité de [Organisation].
2. Toute infraction à cette politique résultera en des actions disciplinaires dans le respect des procédures de [Organisation].

# Avez-vous des questions ?

N’hésitez jamais à prendre contact avec [Helpdesk IT de l’organisation] si :

* vous avez des questions ou des remarques sur cette politique ;
* vous soupçonnez la présence d'incidents ou en avez la confirmation.

Coordonnées :

* [Numéro de téléphone Helpdesk IT de l’organisation]
* [E-mail Helpdesk IT de l’organisation]

# Annexe : Checklist pour la mise en œuvre des dispositions de la politique d'utilisation acceptable

Le tableau suivant indique les principales actions à mettre en œuvre par [Organisation], compte tenu de la politique actuelle. Dans la colonne « Clôturé ? », la personne responsable de la mise en œuvre peut définir le statut approprié (« Oui »/ »Non »/ « N/A »).

| Actions | Clôturé ? |
| --- | --- |
| Veiller à ce que tous les collaborateurs signent la politique d'utilisation acceptable avant de commencer | Choisissez un élément |
| Organiser des formations de sensibilisation des collaborateurs à l’importance de cette politique | Choisissez un élément |
| Partager les informations conformément aux lignes directrices relatives à la classification et au traitement des données | Choisissez un élément |