|  |
| --- |
| **Politique de sécurité de l’information** |
| 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 de 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. Context 3](#_Toc127893363)

[1.1. Purpose of this document 3](#_Toc127893364)

[1.2. Scope of this document 3](#_Toc127893365)

[1.3. Role and responsibilities 3](#_Toc127893366)

[1.4. Definitions 4](#_Toc127893367)

[1.5. Policy enforcement 4](#_Toc127893368)

[2. Policy statements 5](#_Toc127893369)

[2.1. Information classification and handling 5](#_Toc127893370)

[2.2. Information retention and destruction 8](#_Toc127893371)

[2.3. Protection of personal data 8](#_Toc127893372)

[Annex: Explanatory Notes 9](#_Toc127893373)

[Policy specific 9](#_Toc127893374)

[Further reference documentation 10](#_Toc127893375)

# 

# Contexte

Les *informations* peuvent se décliner sous plusieurs types de support : physique (informations imprimées ou écrites, par exemple), électronique (informations stockées ou transmises via des systèmes d'information) et humain (informations détenues par des personnes ou échangées lors de conversations).

Les informations constituent une part essentielle de [Organisation] puisqu’elles représentent les connaissances que nous produisons et qu’elles soutiennent le développement et la continuité de toutes nos opérations.

| Création | Stockage | Traitement | Archivage | Élimination |
| --- | --- | --- | --- | --- |
| * Création * Collecte * Classification * Enregistrement | * Organisation * Stockage | * Consultation * Récupération * Utilisation * Mise à jour * Diffusion | * Rétention | * Suppression * Destruction |

Cette politique de sécurité de l’information résume comment [Organisation] s’efforce de protéger ses informations contre tout accès non autorisé, toute modification ou destruction, et d’assurer leur confidentialité, leur intégrité et leur disponibilité tout au long de leur cycle de vie :

## Objectif de ce document

Le présent document vise à définir l’approche que [Organisation] doit suivre en matière de classification et de gestion des informations et ce, s’agissant de leur création, de leur utilisation autorisée et de leur suppression correcte.

## Champ d’application de ce document

Cette politique s’applique à toutes les informations que les collaborateurs et contractants de [Organisation] utilisent pour interagir avec ces ressources. Elle s’applique aussi au cycle de vie de la gestion des informations dans son ensemble.

## Rôles et responsabilités

Le tableau ci-dessous décrit les rôles de [Organisation]. Chaque rôle des opérations commerciales et de sécurité peut être mis à jour avec les rôles ou les positions de la personne responsable au sein de [Organisation], le cas échéant.

| Rôle | Description |
| --- | --- |
| [Responsable de l’organisation] | La personne appartenant à la direction de [Organisation] responsable de la mise en œuvre de cette politique en interne. |
| [Responsable IT] | Le collaborateur de [Organisation] tenu d'agir conformément à la présente politique en cas de problème de sécurité de l'information. |
| [Helpdesk IT organisation] | Le collaborateur ou l'équipe de [Organisation] chargé(e) d'être le premier point de contact des collaborateurs et des contractants de [Organisation] en cas d'incident lié à la sécurité de l'information. |
| Collaborateurs et contractants | Toutes les personnes fournissant un service professionnel dans le cadre d'un accord légal pour [Organisation]. |
| [Représentant du département] | Toute personne responsable d'un service spécifique des activités de [Organisation]. |
| Tierces parties | Toute personne non salariée de [Organisation] qui est contractuellement tenue de fournir une certaine forme de service à [Organisation]. |
| Parties externes | Toute organisation, association ou organisation juridique externe avec laquelle [Organisation] peut communiquer lorsqu'elle est concernée par la gestion d'un incident lié à la sécurité de l'information. |
| Propriétaire des informations | Le collaborateur ou le représentant du département ayant l'autorité statutaire ou opérationnelle pour établir les règles de traitement et les contrôles applicables aux informations spécifiées. |

## Définitions

Le tableau suivant reprend les définitions de tous les acronymes et termes utilisés dans ce document :

| Terme | Définition |
| --- | --- |
| Disponibilité | La capacité à permettre un accès rapide et fiable aux informations et aux ressources connexes aux utilisateurs autorisés. |
| Confidentialité | Le maintien de l'accès autorisé afin de garantir que les informations et les systèmes ne sont accessibles qu'aux utilisateurs autorisés. |
| Intégrité | La protection contre toute modification ou destruction impropres des informations, en ce compris assurer toute non-répudiation des données et leur authenticité. |
| Cycle de vie des informations | Les étapes par lesquelles passent les informations, généralement la création, le stockage, le traitement, l'archivage et l'élimination. |
| Informations | Toute communication ou représentation de connaissances comme des faits, données ou opinions, quel que soit le support ou la forme, y compris les formes textuelles, numériques, graphiques, cartographiques, narratives, électroniques ou audiovisuelles. |
| Données à caractère personnel | Les données à caractère personnel représentent toutes les informations qui se rapportent à une personne physique identifiée ou identifiable. |

Lors de leur première apparition dans le document, les termes de ce tableau seront indiqués en *italique*.

## Mise en œuvre de la politique

1. Dans les dispositions de la politique, les termes « doit » et « ne doit pas » indiquent une exigence, tandis que les termes « devrait » et « ne devrait pas » indiquent une recommandation.
2. Sans exception formellement approuvée, le non-respect des dispositions de la politique peut faire l'objet de mesures disciplinaires conformément aux politiques et procédures des ressources humaines de [Organisation].
3. Le responsable de l'élaboration de cette politique adaptera toutes les parties du document mises en évidence par des crochets [ ] et surlignées en bleu clair (#60BCCF), en fonction de la structure, du contexte et des besoins de [Organisation].

# Dispositions de la politique

## Classification et traitement des informations

Les collaborateurs doivent classer et traiter les informations selon la manière définie par [Organisation]. La classification des informations est basée sur l'impact potentiel sur la confidentialité, l'intégrité et la disponibilité en cas de divulgation, de modification ou de destruction non autorisée.

L'impact sera considéré faible, modéré ou élevé :

* Faible : La divulgation, modification ou destruction non autorisée d'informations ne devrait avoir qu'un impact limité, voire nul, sur les activités et les actifs de l'organisation ou sur les individus.
* Modéré : La divulgation, modification ou destruction non autorisée d'informations pourrait avoir un impact considérable sur les activités et les actifs de l'organisation ou sur les individus.
* Élevé : La divulgation, modification ou destruction non autorisée d'informations pourrait avoir de graves répercussions sur les activités et les actifs de l'organisation ou sur les individus.

Il existe trois niveaux de classification des informations : confidentiel, interne et public. Ces niveaux sont définis ci-dessous, accompagnés d'exemples et d'un guide d’utilisation. Il incombe à tous les collaborateurs et contractants de prendre connaissance de ces niveaux de classification, de comprendre ce qu'ils impliquent et d’agir en conséquence.

| **Niveau** | **Description** | **Guide d’utilisation** |
| --- | --- | --- |
| **Confidentiel** | Seul un nombre restreint de collaborateurs ayant une fonction spécifique peut avoir accès aux informations confidentielles. C’est le management, le département ou le type de projet qui détermine les collaborateurs qui peuvent y avoir accès. Voici quelques exemples :   * informations personnelles RH ou dossiers de collaborateurs ; * documents financiers ou contractuels ; * documents légaux, liés à une procédure juridique ou qui font l’objet d'un accord de non divulgation ; * secrets commerciaux ; * documents et prévisions budgétaires. | * Les informations confidentielles doivent uniquement être distribuées moyennant le consentement explicite de leur propriétaire. * Les informations confidentielles doivent uniquement être stockées dans des dossiers ou emplacements prévus à cet effet et être protégés à l’aide de droits d’accès uniquement octroyés aux utilisateurs autorisés. * Les informations confidentielles doivent être cryptées lorsqu’elles ne sont pas utilisées ou en transit. * Une étiquette de classification des informations et le nom du propriétaire doivent figurer sur chaque document confidentiel afin de les identifier correctement. * Les exigences relatives aux informations internes s'appliquent également aux informations confidentielles. |
| **Interne** | Les informations internes sont uniquement destinées aux collaborateurs de [Organisation]. Seules les personnes travaillant pour l’organisation (les collaborateurs, les contractants actifs, etc.) peuvent avoir accès à ces données, selon leurs besoins. Ce type d’informations ne devra pas être partagé librement à des personnes externes à l’organisation, au vu de leur confidentialité et/ou des obligations contractuelles ou légales qui les entourent.  Voici quelques exemples :   * business plans et autres stratégie ; * e-mails ou mémos internes ; * plateformes Intranet de l’organisation. | * Les informations internes doivent stockées à l’aide de services ou plateformes contrôlés ou approuvés. * Les informations internes doivent uniquement être distribuées en interne, moyennant le consentement explicite de leur propriétaire. * Il convient d’utiliser un service de courrier approuvé pour transporter des équipements contenant des informations internes en dehors de [Organisation]. * Les informations internes doivent être supprimées des imprimantes, copieurs et scanners le plus rapidement possible, afin d’éviter toute divulgation non autorisée. |
| **Public** | Les informations publiques sont des informations auxquelles tout le monde peut accéder. Ce sont des informations libres d’accès qui peuvent ainsi être utilisées, réutilisées et partagées sans restriction.  Voici quelques exemples :   * communiqués de presse ; * comptes annuels publiés ; * brochures. | * N/A |

Afin de traiter efficacement les informations de [Organisation] :

1. Les informations doivent être gérées correctement, de leur création jusqu'à leur suppression appropriée, en passant par leur utilisation autorisée.
2. Toutes les informations doivent être classées en permanence en fonction de leurs caractéristiques de confidentialité, d'intégrité et de disponibilité.
3. Une section de contrôle des documents devrait se charger d’identifier le propriétaire des informations et l'étiquette de classification de manière structurelle dans les documents pertinents.
4. Toutes les informations créées, stockées ou traitées dans le cadre d'activités professionnelles doivent uniquement être utilisées aux fins professionnelles prévues.
5. Toutes les informations doivent être liées à un propriétaire.
6. Le propriétaire des informations doit déterminer la classification des informations, ainsi que la manière dont elles seront utilisées et par qui.
7. Le propriétaire des informations doit comprendre l'utilisation des informations dont il est responsable, les risques associés, ainsi que les lois, règlements ou politiques qui en régissent l'accès et l'utilisation.
8. Le propriétaire des informations doit faire preuve de prudence en ce qui concerne la classification correcte des données et ce, afin d'éviter toute divulgation et tout accès inappropriés.
9. Tous les collaborateurs et contractants de [Organisation] doivent recevoir des directives de formation et des documents de sensibilisation en matière de classification des informations.
10. Toute suspicion ou confirmation d’incident de classification, de modification non autorisée, de divulgation ou de destruction des informations de [Organisation] doit être immédiatement signalé au propriétaire des informations désigné et [Helpdesk IT de l’organisation].

## Conservation et destruction des informations

1. La conservation des informations doit être conforme aux exigences réglementaires (comme le RGPD) et commerciales en vigueur.
2. Les propriétaires des informations devraient être consultés avant la destruction des informations.
3. Les propriétaires des informations peuvent prolonger la date d’expiration des informations, en fonction des besoins de l'entreprise et/ou des exigences relatives à la prolongation de la conservation.
4. Les informations de [Organisation] qui ne sont plus nécessaires doivent être supprimées de manière sécurisée (par exemple déchiquetées ou par l'intermédiaire d'un fournisseur tiers de confiance).
5. Tous les collaborateurs de [Organisation] doivent connaître le processus de destruction des données de [Organisation] (les techniques de destruction physique pour les supports optiques et les bandes, ainsi que l'effacement des données stockées sur des disques durs et disques SSD).
6. Seuls les collaborateurs autorisés et formés à cet effet doivent détruire les informations et les biens confidentiels.

## Protection des données à caractère personnel

1. Les *données à caractère personnel* relatives à une personne identifiée ou identifiable (nom, adresse, adresse mail, numéro de registre national ou informations médicales) doivent être classées « confidentielles ».
2. La collecte, l’utilisation et la détention de données à caractère personnel devraient être restreintes et limitées aux informations strictement nécessaires à la réalisation de ses missions, avec un délai d'expiration qui n'excède pas les besoins de l'entreprise et, le cas échéant, conformément à la politique de confidentialité de [Organisation].

# Annexe : Notes explicatives

## Concernant la politique

Le résumé ci-dessous des tâches et des principaux rôles suggérés en matière de sécurité de l'information. Sur cette base, chaque organisation peut attribuer le type de niveau de responsabilité conformément à la légende ci-dessous. Des rôles supplémentaires peuvent être attribués, le cas échéant, pour les tâches énumérées dans le tableau ci-dessous.

|  |  |
| --- | --- |
| **R** | Responsible |
| **A** | Accountable |
| **C** | Consulted |
| **I** | Informed |

Des rôles supplémentaires peuvent être attribués en fonction des responsabilités reprises dans la liste.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rôle**  **Tâche** | **[Responsable de l’organisation]** | **[Responsable IT]** | **Propriétaire des informations** | **Helpdesk IT organisation** | **Collaborateurs et contractants** | **Représentants du département** | **[Autre rôle]** |
| Informer les collaborateurs et contractants quant aux exigences en termes de classification des informations | **[A]** | **[C]** | **[R]** | **[C]** | **[I]** | **[C]** |  |
| Revoir à titre périodique cette politique et les politiques, lignes directrices et procédures qui y sont liées. | **[A]** | **[C]** | **[R]** | **[C]** |  | **[C]** |  |
| Définir un délai de détention de toutes les informations de [Organisation], en ce compris les données à caractère personnel. | **[A]** | **[C]** | **[R]** |  |  | **[C]** |  |
| Revoir la conformité avec les lois et législations pertinentes (comme le RGPD). | **[A]** | **[C]** | **[R]** |  |  | **[C]** |  |
| Développer un canevas pour identifier le propriétaire des informations et l’étiquette de classification dans les documents pertinents. | **[A]** | **[C]** | **[R]** | **[C]** |  | **[C]** |  |
| Définir le processus de destruction pour chaque type d'information. | **[A]** | **[C]** | **[R]** | **[C]** |  | **[C]** |  |

## Documentation de référence supplémentaire

Le tableau ci-dessous présente d'autres documents pouvant aider à la mise en œuvre de la politique :

|  |  |
| --- | --- |
| **Titre** | **Lien vers documentation (si disponible)** |
| Classification des informations | <https://cert.be/en/traffic-light-protocol-tlp> |
| NIST Cyber Security Framework : | https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf |
| [Indiquer les documents et procédures de [Organisation] |  |