|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | Politique de gestion des incidents liés à la sécurité de l’information | | Organisation : [Organisation] | | Classification des informations : [Catégorie] |   Contrôle document   |  |  |  |  | | --- | --- | --- | --- | | Version | Mis à jour par | Date | Description des changements | | 1.0 | [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. Context 3](#_Toc126850226)

[1.1. Purpose of this document 3](#_Toc126850227)

[1.2. Scope of this document 3](#_Toc126850228)

[1.3. Roles and Responsibilities 3](#_Toc126850229)

[1.4. Definitions 4](#_Toc126850230)

[1.5. Policy Enforcement 4](#_Toc126850231)

[2. Policy statements 5](#_Toc126850232)

[2.1. Responsibilities and procedures 5](#_Toc126850233)

[2.2. Preparing for information security incidents 5](#_Toc126850234)

[2.3. Detecting information security incidents 5](#_Toc126850235)

[2.4. Reporting of information security incidents 5](#_Toc126850236)

[2.5. Response to information security incidents 6](#_Toc126850237)

[2.6. Collection of evidence 6](#_Toc126850238)

[2.7. Learning from information security incidents 6](#_Toc126850239)

[Annex: Explanatory Notes 7](#_Toc126850240)

[Policy specific 7](#_Toc126850241)

[Further reference documentation 11](#_Toc126850242)

# Contexte

Les incidents de sécurité de l'information constituent une menace considérable en raison de l'impact qu'ils sont susceptibles d’exercer sur nos activités (par exemple, capacités, réputation) et nos fonctions organisationnelles (par exemple, personnel, infrastructure, logiciels). L'objectif de la gestion des incidents est de rétablir le fonctionnement normal des services le plus rapidement possible et d'atténuer l'impact négatif sur les activités.

La gestion des incidents vise les objectifs suivants :

* Organiser la collecte et la détection des événements et incidents liés à la sécurité de l'information ;
* Confirmer si un incident est réellement survenu ;
* Élaborer un processus de notification des incidents défini ;
* Promouvoir la collecte et la documentation d’informations précises ;
* Mettre en place des contrôles pour la récupération et le traitement appropriés des éléments de   
  preuve ;
* Contenir l'incident et mettre fin à toute activité indésirable de manière rapide et efficace ;
* Minimiser la perturbation des opérations ;
* Présenter des rapports précis et des recommandations utiles à la direction ; et
* Prévenir et/ou atténuer les incidents futurs.

## Objectif de ce document

Ce document a pour objectif de définir l'approche que [Organisation] doit adopter afin de se préparer aux incidents de sécurité de l’information, de les détecter et d’y répondre. Il entend assurer que [Organisation] se prépare aux incidents liés à la sécurité de l’information, les identifie, les contienne, les étudie, y remédie, en fasse rapport et y réagisse adéquatement.

## Champ d'application de ce document

Cette politique s'applique aux incidents de sécurité de l’information qui affectent les informations, les systèmes IT (Information Technology), les infrastructures et les personnes. Elle concerne en outre l’ensemble du cycle de vie de la gestion des incidents de sécurité de l’information, y compris le signalement et l’évaluation des incidents de sécurité de l’information, la réponse apportée, la communication autour de ces incidents et les enseignements à en tirer, qu'ils soient potentiels ou confirmés. Cette politique s'applique à toutes les informations et fonctions de [Organisation] , avec pour cible les collaborateurs et les contractants impliqués dans le traitement des incidents de sécurité de l'information.

## Rôles et responsabilités

Le tableau suivant reprend les rôles au sein de [Organisation], ainsi que leur description. Chaque rôle des opérations commerciales et de sécurité peut être mis à jour avec les rôles ou les positions de la personne responsable, 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 de sécurité de l'information. |
| Collaborateurs et contractants | Tout le personnel fournissant un service d’ordre professionnel dans le cadre d'un accord légal pour [Organisation]. |
| [Représentants du département] | Toute personne responsable d’un département spécifique des activités de [Organisation]. |
| Tierces parties | Toute personne non employée par [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 de sécurité de l'information. |

## Définitions

Le tableau suivant définit tous les acronymes et concepts utilisés dans ce document :

| Concept | Définition |
| --- | --- |
| Incident de sécurité de l’information | Un évènement isolé ou une série d'événements de cybersécurité non désiré(s) ou inattendu(s) susceptible(s) de compromettre les activités de l'organisation. |
| Root Cause Analysis (RCA - analyse des causes profondes) | Approche consistant à enquêter sur la cause sous-jacente d'un incident afin que des mesures appropriées puissent être prises pour éviter que l'incident ne se reproduise. |
| Mesures d’atténuation | Contrôle mis en place pour protéger les systèmes informatiques, les données et les applications contre les cybermenaces. Les mesures peuvent comprendre la prévention, la détection et la réponse à de telles attaques. |
| Vulnérabilité | Un défaut ou une faiblesse dans un système informatique, ses procédures de sécurité, ses contrôles internes ou sa conception et sa mise en œuvre, susceptible d’être exploité(e) pour violer la politique de sécurité du système. |

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. Toutes les parties du document indiquées à l'intérieur de [ ] et surlignées en bleu clair (#60BCCF) doivent être adaptées par le responsable de l'élaboration de cette politique en fonction de la structure, du contexte et des besoins de [Organisation].

# Dispositions de la politique

## Responsabilités et procédures

1. Les procédures de gestion des incidents de sécurité de l'information doivent être documentées, mises en œuvre et tenues à jour.
2. Les procédures de gestion des incidents de sécurité de l'information doivent couvrir au minimum les éléments suivants :

* Un plan de réponse aux incidents détaillant la manière d'analyser, de contenir et d'éradiquer les *incidents de sécurité de l'information,* d’en récupérer et d’en tirer des enseignements ;
* Des procédures de traitement et de signalement des incidents, y compris le signalement de preuves aux autorités, et des manuels de simulation d'incidents liés à la sécurité de l'information ;
* Des lignes directrices en matière de communication interne et externe, y compris les principes de la communication de crise ;
* Des lignes directrices en matière de formation, y compris pour les exercices de simulation.

1. Les rôles et responsabilités doivent être clairement définis pour chaque procédure.
2. Les informations relatives aux incidents de sécurité de l'information doivent être traitées de manière confidentielle.
3. Le [Responsable IT] doit informer tous les collaborateurs et contractants de [Organisation] des actions à prendre en cas d’incident de sécurité de l’information.
4. Les [Représentants du département] doivent fournir les coordonnées de leurs représentants primaires et secondaires et notifier immédiatement tout changement dans ces informations.
5. La procédure de signalement des incidents de sécurité de l'information doit être simple, claire, accessible et facilement disponible pour le public visé (y compris les collaborateurs, les contractants, les clients et le public).

## Préparation aux incidents de sécurité de l’information

1. L'escalade des incidents doit être simple et directe et intégrer une ligne de communication directe entre le [Responsable IT] et le [Responsable de l’organisation] en cas d’incidents significatifs.
2. Des critères permettant de déterminer à quel moment un incident de sécurité de l'information passe au stade de crise devraient être définis (par exemple, sur la base de l'impact sur les services commerciaux ou de la période d'indisponibilité des services informatiques).
3. Les rôles et responsabilités des parties externes ou fournisseurs en cas d’incidents de sécurité de l’information devraient être clarifiés, particulièrement en ce qui concerne le support.
4. Des cas pratiques pour les menaces et les *vulnérabilités* les plus courantes devraient être définis afin de surveiller les événements spécifiques liés à la sécurité de l'information.
5. Des simulations d'incidents de sécurité de l'information devraient être testées périodiquement, au moins une fois par an, afin de permettre une réponse efficace de la part de [Organisation], du personnel et du [Helpdesk IT de l’organisation]. Les enseignements tirés doivent être documentés et utilisés pour améliorer encore l'efficacité de la réponse aux incidents.
6. Le personnel de [Organisation] et le [Helpdesk IT de l’organisation] devraient disposer de manuels de simulation d'incidents liés à la sécurité de l'information afin d'atténuer les incidents les plus courants (par exemple, les ransomwares).

## Détection des incidents liés à la sécurité de l’information

1. Les alertes des systèmes, les vulnérabilités et les actions des utilisateurs doivent être enregistrées dans un fichier journal pour suivre les incidents liés à la sécurité de l'information.
2. Les alertes, les vulnérabilités et les journaux des systèmes devraient faire l’objet d’un monitoring afin de détecter activement les incidents liés à la sécurité de l'information.

## Signalement d’incidents liés à la sécurité de l’information

1. Les collaborateurs et les contractants de [Organisation] doivent signaler immédiatement tout incident lié à la sécurité de l’information suspect ou avéré au [Helpdesk IT de l’organisation] via [Adresse e-mail ; Numéro de téléphone ; URL du système de tickets].
2. Le [Responsable IT] doit informer tous les collaborateurs et contractants de tout élément considéré comme un incident lié à la sécurité de l’information, de leur devoir de signaler tout incident lié à la sécurité de l’information, ainsi que du mode de signalement et de la personne à qui faire rapport.
3. Les rapports adressés au [Responsable de l’organisation] devraient comprendre un résumé des incidents de sécurité de l'information, la cause profonde, les fonctions commerciales et informatiques touchées, ainsi que les mesures proposées et les mesures correctrices prises.
4. L'impact des incidents de sécurité de l'information doit être classé selon une échelle [Critique ; Important ; Moyen ; Faible ] afin de faciliter une escalade appropriée. Si l'incident de sécurité de l'information fait partie d'une violation de données à caractère personnel, cela devrait être indiqué dans le signalement.
5. Le statut de l'incident doit être suivi et mis à jour au moins pour les incidents de sécurité de l'information significatifs avec les catégories [En attente ; Confirmé ; Résolu] tout au long de leur cycle de vie.
6. Le [Helpdesk IT de l’organisation] devrait fournir un feedback aux personnes qui ont signalé l'incident de sécurité de l'information lorsque le statut de l'incident de sécurité de l'information est [Confirmé] et [Résolu].

## Réponse aux incidents liés à la sécurité de l’information

1. Tous les incidents confirmés en matière de sécurité de l'information doivent être traités conformément au plan de réponse aux incidents qui détaille la manière d'analyser, de contenir et d'éradiquer les incidents, d’en récupérer et d’en tirer des enseignements.
2. Les incidents de sécurité de l'information [Critiques] doivent être communiqués au [Responsable de l’organisation] et au [Responsable IT].
3. Seules les personnes autorisées doivent assurer la communication d'incidents de sécurité de l'information à des parties externes.
4. Le signalement des incidents de sécurité de l'information aux parties externes concernées [Autorité de protection des données, Police, Fédération sectorielle] doit respecter la loi ou la réglementation.

## Collecte de preuves

1. Les preuves d'un incident de sécurité de l'information susceptibles de donner lieu à une action en justice doivent être collectées, conservées et présentées de manière à satisfaire aux exigences d'admissibilité et de poids de la preuve dans la ou les juridiction(s) concernée(s).
2. La protection des preuves collectées doit être conforme aux procédures de gestion des accès et à toutes les exigences légales applicables. Une protection appropriée doit consister en un cryptage, un stockage sécurisé et des restrictions d'accès aux preuves collectées lors d'incidents liés à la sécurité de l'information.

## Enseignements tirés des incidents liés à la sécurité de l’information

1. Les incidents de sécurité de l’information avérés doivent faire l’objet d’une analyse afin d’en découvrir les causes profondes (au moins pour les incidents de sécurité de l’information récurrents et/ou significatifs).
2. Les rapports d'incidents significatifs en matière de sécurité de l'information doivent être transmis périodiquement au [Responsable de l’organisation] et indiquer le type, le volume et l'impact de l’incident et les enseignements tirés.
3. Tous les collaborateurs et contractants de [Organisation] doivent être formés à la gestion des incidents de sécurité de l'information pour réduire la probabilité ou l'impact d'incidents de sécurité de l'information récurrents ou à impact majeur.
4. Un monitoring des systèmes d'information doit être mis en place pour réduire la probabilité ou l'impact des incidents de sécurité de l'information récurrents ou ayant un impact significatif.
5. *L'analyse des causes profondes* doit conduire à l'identification de *mesures d'atténuation.*

# **Annexe : Notes explicatives**

## Concernant la politique

La politique de gestion des incidents liés à la sécurité de l'information aide les organisations à définir les activités requises pour traiter les différents types d'incidents. Elle fournit la structure et les outils procéduraux nécessaires pour réagir aux incidents de sécurité de l’information, les signaler et les atténuer avant qu'ils n'aient un impact sur les actifs les plus importants de l'organisation d'un point de vue commercial et opérationnel, ainsi que pour prévenir les conséquences juridiques.

La politique de gestion des incidents de sécurité de l'information est généralement complétée par une procédure de réponse à l'incident ou un manuel qui sert de plan d'action descriptif pour répondre aux menaces qui pèsent sur l'organisation (cfr. [Procédure de réponse aux incidents]).

### Rôles et responsabilités

Pour soutenir la mise en œuvre de cette politique et implémenter les rôles identifiés dans la section 1.3. Rôles et responsabilités, veuillez vous référer à l'aperçu suivant reprenant les tâches de gestion de réponse aux incidents suggérées et les rôles principaux. 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 |

L’on peut attribuer des rôles supplémentaires en fonction des responsabilités épinglées. La première tâche a été assignée à titre d’illustration.

| Rôle  Tâche | [Responsable de l’organisation] | [Responsable IT] | Helpdesk IT de l’organisation | Collaborateurs et contractants | Représentants du département | [Autre rôle] |
| --- | --- | --- | --- | --- | --- | --- |
| Maintenance des procédures de gestion des incidents de sécurité de l’information | **[A]** | **[R]** | **[C]** |  |  |  |
| Information des collaborateurs et des contractants des mesures à prendre à la suite d'un incident de sécurité de l'information | **[A]** | **[R]** |  |  | **[I]** |  |
| Fourniture de coordonnées pertinentes aux représentants primaires et secondaires désignés | **[A]** | **[R]** |  |  |  |  |
| Gestion des demandes d’escalade des incidents | **[A]** | **[R]** | **[C]** |  |  |  |
| Réalisation de simulations et de tests périodiques concernant les incidents de sécurité de l’information | **[A]** | **[R]** | **[I]** |  |  |  |
| Signalement interne de tout incident de sécurité de l’information suspect ou avéré | **[A]** | **[R]** | **[C]** |  | **[I]** |  |
| Information des collaborateurs et des contractants des mesures en vue du signalement des incidents de sécurité de l'information | **[A]** | **[R]** | **[I]** |  | **[I]** |  |
| Traitement, classification de l'impact, suivi et mise à jour de l'incident de sécurité de l'information | **[A]** | **[R]** | **[C]** |  |  |  |
| Feedback aux personnes qui ont signalé les incidents de sécurité de l’information | **[A]** | **[R]** |  |  | **[I]** |  |
| Communication d’incidents de sécurité de l’information aux parties externes | **[A]** | **[R]** |  |  | **[I]** |  |

### Statut du ticket

Le tableau suivant vient compléter la section [2.4. Signalement d’incidents de sécurité de l’information](#_Reporting_of_information_1) en indiquant les statuts potentiels des tickets de réponses aux incidents :

|  |  |
| --- | --- |
| Statut | Description |
| En attente | Une demande portant le statut « en attente » signifie que le système a reçu la demande de signalement. |
| Confirmé | La demande de signalement a été acceptée et est examinée pendant que l'on travaille sur l'incident signalé. |
| Résolu | L’incident signalé introduit par une demande de signalement a été résolu avec succès. |

### Fonctions organisationnelles

Le tableau suivant vient compléter la section [2.4. Signalement d’incidents de sécurité de l’information](#_Reporting_of_information_1) avec mention d’exemples de fonctions organisationnelles :

|  |  |
| --- | --- |
| Type | Description |
| Infrastructure | Fonction incluant les structures et équipements physiques et organisationnels de base de [Organisation]. |
| Personnel | Fonction incluant toutes les personnes employées par [Organisation]. |
| Logiciel | Fonction incluant des programmes et autres systèmes d’exploitation utilisés par [Organisation]. |

### Niveau de classification des incidents de sécurité de l’information

Le tableau suivant vient compléter la section [2.4. Signalement d’incidents de sécurité de l’information](#_Reporting_of_information_1) en l’illustrant par des exemples de niveaux de classification d’incidents :

|  |  |
| --- | --- |
| Niveau | Description |
| Critique | Les incidents de sécurité de l’information de la catégorie « critique » affectent [Organisation] dans son ensemble, en compromettant la fonctionnalité de toute l’organisation. |
| Important | Les incidents de sécurité de l’information relevant de la catégorie « important » affectent plusieurs fonctions de [Organisation], en compromettant la fluidité du fonctionnement de l’organisation. |
| Moyen | Les incidents de sécurité de l’information relevant de la catégorie « moyen » affectent des fonctions secondaires de [Organisation], avec un impact modéré sur les processus de l’organisation. |
| Faible | Les incidents liés à la sécurité de l’information de la catégorie « faible » n’ont qu'un impact réduit et d’intérêt secondaire sur [Organisation], sans compromettre la fonctionnalité de l’organisation. |

### Mesures de réduction de l’impact des incidents liés à la sécurité de l’information

Le tableau ci-dessous présente des exemples de mesures de réduction mentionnées dans la section [2.7 Enseignements tirés des incidents liés à la sécurité de l’information](#_Learning_from_information)  qui peuvent être mises en œuvre pour réduire l'impact des incidents de sécurité de l'information :

|  |  |
| --- | --- |
| Mesure de sécurité | Description |
| Formation de sensibilisation à la sécurité | Veiller à ce que tous les collaborateurs et contractants de l'organisation aient une connaissance suffisante de la sécurité pour en comprendre la nécessité et pour être vigilants, dans leur travail quotidien, à l'égard des dangers liés à la sécurité. Prévoir des formations régulières en matière de sécurité pour tous les collaborateurs et contractants. |
| Évènements d’audit | Veiller à ce que l'activité sur le système laisse une trace qui permette de mener des enquêtes fiables sur les incidents de sécurité de l'information après leur survenance. Protéger les dossiers contre tout accès non autorisé et les réviser périodiquement. |
| Protection cryptographique | Fournir des propriétés de sécurité en transformant les informations en formules mathématiques, utiliser les formules cryptographiques appropriées pour protéger toutes les informations de l'organisation classées comme nécessitant une protection. |
| Partage d'informations | Aider les collaborateurs et contractants autorisés à prendre des décisions qui assurent la sécurité du partage d'informations avec des partenaires. Permettre aux collaborateurs et contractants de déterminer si le destinataire d'une information est autorisé à y accéder. Permettre aux collaborateurs et contractants de prendre des décisions en matière de partage d'informations au moyen de mécanismes automatisés ou de processus manuels. |
| Évaluation de la sécurité | Évaluer périodiquement les contrôles de sécurité du système afin de déterminer dans quelle mesure les contrôles sont mis en œuvre correctement, fonctionnent comme prévu et produisent le résultat escompté, et communiquer le résultat de l'évaluation aux personnes ou rôles prédéfinis au sein de l'organisation. |

## Documentation de référence supplémentaire

Le tableau suivant présente d'autres documents qui peuvent aider à la mise en œuvre de la politique :

|  |  |
| --- | --- |
| Titre | Lien vers la documentation (si disponible) |
| Classification des informations | <https://cert.be/fr/le-traffic-light-protocol-tlp> |
| Centre pour la cybersécurité Belgique Cyber Security Incident Management Guide | <https://ccb.belgium.be/fr/document/cyber-security-incident-management-guide> |
| Signalement des incidents | <https://www.safeonweb.be/en/useful-links> |
| NIST Cyber Security Framework :  ID.GV Governance  DE.DP Detection Processes  RS.AN Analysis  RS.CO Communications  RS.RP Response Planning  RC.IM Improvements | https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf |
| [Indiquer les documents et procédures de l'[Organisation]] |  |