CENTRE FOR
CYBER SECURITY
BELGIUM

Baseline Information Security Guidelines (BSG)
Édition 2018

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

CHANCELLERY OF
THE PRIME MINISTER

.be

CENTRE FOR
CYBER SECURITY
BELGIUM

Introduction

Aujourd'hui, nul ne doute que les Technologies de l'Information et de la Communication (TIC) jouent un rôle important dans la vie économique et sociale. Le bon fonctionnement des réseaux, des systèmes informatiques et des logiciels revêt une importance capitale pour les institutions publiques, les organisations qui dépendent largement de leur infrastructure TIC et, par conséquent, du personnel qui en assure le bon fonctionnement.

L'objectif du présent document, "Baseline Security Guidelines (BSG)", est de fournir aux administrations publiques des lignes directrices minimales, sous forme de guide, pour toute implémentation ou évaluation d'un plan de sécurité de l'information afin d'aider les responsables de traitement soutenus par la direction ainsi que les professionnels dans la gestion de l'information (conseillers en sécurité, responsables informatiques, etc.).

Il n'est donc pas dans l'intention de développer une ligne directrice complète et approfondie, car elle existe déjà.

Ce BSG a été élaboré en collaboration avec des experts de différents SPF et des experts externes en tenant compte des standards existants en la matière comme l'ISO 27001 et l'ISO 27002.

S'il existe de nombreux cadres référentiels ("frameworks") concernant la sécurité de l'information, l'utilisation de la norme ISO 2700X comme point de départ présente assurément une valeur ajoutée. Une organisation utilisant un autre cadre peut facilement évaluer si les mesures mises en place sont compatibles avec les directives minimales reprises dans ce document.

Il est également important de mentionner que ces lignes directrices et ce cadre pour la sécurité de l'information ne sont pas indépendants, car ils font partie intégrante de la gestion d'entreprise dans sa globalité.

Cela signifie que de nombreuses activités décrites ci-dessous, telles que la gestion des risques, la communication, l'audit et le contrôle et l'amélioration continue, peuvent être réutilisées ou intégrées dans des cadres existants.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

CENTRE FOR
CYBER SECURITY
BELGIUM

Table des matières

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

CHANCELLERY OF
THE PRIME MINISTER

.be

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

1 Les quatre principes de base d'une gestion de la sécurité de l'information

Il convient de garder à l'esprit **quatre principes** clefs lors de la mise en place d'une bonne gestion de la sécurité de l'information, à savoir:

1. La stratégie et le soutien de la direction
2. L'inventaire des actifs et l'analyse des risques
3. La mise en place des mesures de sécurité
4. L'évaluation des mesures de sécurité

L'évaluation des mesures de sécurité Ces principes de base s'inspirent d'une approche de qualité de la sécurité de l'information qui consiste à continuellement évaluer les actions mises en œuvre afin d'améliorer la qualité (PDCA = Plan, Do, Check, Act).

Important

Après l'implémentation initiale du plan PDCA, l'évaluation continue devient un cycle répétitif dans le but d'améliorer la sécurité.

Ces principes contiennent **15 points d'attention** qui sont les suivants.

1.1 La stratégie et le soutien de la direction

1. **L'implication des dirigeants et des responsables de traitement** est la meilleure façon de soutenir la mise en place de structures opérationnelles, de procédures et de moyens. Cependant, afin que les moyens mis en œuvre soient efficaces, il convient de les communiquer à toutes les parties prenantes de votre organisation.
2. Développer une **stratégie en matière de sécurité (politique de sécurité)** de l'information en adéquation avec la stratégie de l'organisation afin qu'elle supporte les objectifs tout en respectant les dispositions légales et règlementaires.
3. Définir un plan pluriannuel de **formations et de sensibilisation** régulières pour l'ensemble des collaborateurs internes et externes et de l'organisation.
4. Intégrer pour tout nouveau **projet une culture de sécurité** et d'analyse de risques dès le début, que ce soit au niveau du développement de nouvelles applications ou de projets de gestion de l'entreprise.
5. Disposer d'un plan de gestion des **incidents de sécurité** majeurs/graves et de crises.
6. Mener une **gestion active et régulière des changements importants** de l'environnement.
7. Disposer d'**un plan de continuité des activités** (PCA).

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

1.2 L'inventaire des actifs et l'analyse des risques

8. **Identifier les actifs essentiels de l'information** ainsi que leur propriétaire, et ensuite définir les rôles et responsabilités pour toute la chaîne de traitement du risque.
9. **Gérer les risques** pour définir les priorités et mettre en place les mesures appropriées afin de réduire les risques (en les ramenant à un niveau acceptable) et les impacts potentiels liés aux actifs d'information.

1.3 La mise en place des mesures de sécurité

10. Mettre en place **des mesures spécifiques** visant à la sécurisation de l'information de l'organisation qui doivent être validées, communiquées, implémentées et revues.
11. **Gérer les ressources** allouées à la sécurité de l'information et aux infrastructures de façon efficace et efficiente, en ce compris la désignation de responsables de la sécurité de l'information.
12. Mettre en place, avec le soutien de la direction, **une politique de catégorisation des systèmes d'information et des données sensibles** sur la base des principes de confidentialité, d'intégrité et de disponibilité (de l'anglais "*Confidentiality, integrity and availability*" ou *CIA*) et ce, pour toute leur durée de vie. Cette politique devra faire l'objet d'une révision périodique.

1.4 Evaluation des mesures de sécurité

13. **Effectuer une évaluation annuelle des mesures de sécurité** afin d'évaluer l'état des lieux sur l'avancement du plan de sécurité, ses améliorations et ajouts éventuels est nécessaire pour toute organisation.
14. **Mesurer**, de façon ponctuelle, **les performances des actions** (points précédents) mises en place mais également l'évolution des menaces et des vulnérabilités afin de s'assurer que les objectifs sont atteints (cycle d'amélioration continue, PDCA)
15. Envisager d'**adapter l'analyse et la gestion des risques** à la lumière des audits et des incidents avérés et des changements importants impactant les activités.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

2 La stratégie et le soutien de la direction

2.1 L'implication des dirigeants

Le plan de sécurité et ses priorités doivent être présentés, approuvés, validés et soutenus par **la direction de l'organisation** comme responsable final de la sécurité de l'information.

Pour ce faire, chaque mesure proposée devra comporter une mention de sa priorité et des ressources nécessaires.

Il est important de vérifier que ce plan est en adéquation avec la **stratégie et les objectifs opérationnels de votre organisation**, sans quoi il sera rejeté par la direction.

Dans la présentation à la direction, il faut veiller à mentionner le niveau de sécurité actuel et le niveau désiré après implémentation du plan. La responsabilité de la direction doit être soulignée, et notamment quant à son acceptation du risque.

Ce plan, une fois approuvé par la direction, devra être intégré aux priorités opérationnelles de l'organisation et être communiqué à l'ensemble de l'organisation et à ses parties prenantes afin d'en obtenir la collaboration.

2.2 La stratégie de la sécurité

La gestion de la sécurité de l'information exige que la direction s'implique, promeuve une culture propice à la sécurité et fasse l'apologie des bonnes pratiques et des mesures de sécurité.

Néanmoins, même s'il est plus facile d'acheter une solution technique que d'essayer de changer la culture de l'organisation, n'importe quelle solution technique ne battra pas **l'efficacité et la créativité d'une solution humaine**.

La gestion de la sécurité de l'information fait partie de toute bonne gestion de l'organisation. Elle fournit aux dirigeants une direction stratégique. Elle s'assure en outre que les objectifs sont atteints, que les risques sont gérés de façon appropriée et que les ressources opérationnelles sont gérées efficacement. Elle mesure aussi la réussite et/ou l'échec du programme de sécurité.

Une identification des rôles et responsabilités de chacun quant à la protection de l'information ainsi que la structure de l'organisation sont des outils indispensables afin de permettre une évaluation des tâches et activités nécessaires à la mise en place de ce plan (définition d'une matrice RACI p.ex.).

Afin d'obtenir une gestion de l'information efficace, il importe que la direction en fixe le cadre afin de guider son développement ainsi que la réalisation du plan de sécurité de l'information.

Ceci permettra à l'organisation de gérer ses actifs essentiels (infrastructure, données, …) tout en les protégeant de risques importants.

Afin d'améliorer l'alignement de cette stratégie sur les objectifs de l'organisation, la stratégie opérationnelle devra fournir les éléments clés pour l'analyse de risques comme, par exemple, les procédures opérationnelles et

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

les ressources critiques pour la stratégie de sécurité de l'information.

Les mesures de sécurité sont la résultante de l'analyse de risques et définissent les grandes lignes du programme de sécurité de l'organisation: les ressources nécessaires, les contraintes, …

Le développement du programme de sécurité de l'information devra également prévoir des outils d'évaluation des mesures mises en place, de leur révision et d'adaptation si nécessaire.

Un **rapport complet et régulier de l'état d'avancement** aux dirigeants permettra de décider d'adaptations et de mesures correctives afin d'atteindre l'état de sécurité souhaité par la stratégie de l'organisation.

L'information aux dirigeants leur permettra d'évaluer les ressources nécessaires pour la sécurité de l'information et donc d'accepter les mesures minimales à prendre pour s'assurer de la sécurité de l'information.

Ces mesures minimales sont adaptées au niveau d'importance des actifs à protéger et à leur degré de sensibilité. Ces mesures de base sont définies en termes de ressources, de procédures et de moyens techniques ; elles sont souvent inspirées de standards ainsi que du respect des lois et règlements nationaux et sectoriels.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

3 Inventorier vos actifs essentiels & l'analyse de risques

3.1 Définition des actifs

On entend par actifs essentiels les actifs ayant de la valeur pour l'organisation et nécessitant des mesures de protection. Les actifs ne se limitent pas uniquement à l'infrastructure IT ou à des moyens tangibles, mais ils s'appliquent aussi à des personnes et des moyens intangibles comme des processus, des procédures, la connaissance et l'expertise.

3.2 L'inventaire des actifs

La première étape **consiste à dresser un inventaire des biens essentiels** au fonctionnement de votre organisation.

Il est recommandé de commencer par exemple par les "actifs essentiels" connus et identifiés par la direction.

La priorité devra être donnée à ceux qui sont indispensables au fonctionnement de votre organisation.

Les différentes itérations de votre plan vous permettront d'enrichir progressivement cet inventaire, de le compléter, de l'étoffer.

3.2.1 Les étapes

Afin de dresser l'inventaire:

- Définissez/identifiez, en collaboration avec la direction et les départements, les différents "actifs essentiels" ;
- Au besoin, rencontrez les personnes responsables de ces différents actifs afin de mieux les cerner/définir ;
- Dressez-en la liste ;
- Soumettez cette liste, de façon formelle, à la direction pour approbation. Cela permettra de l'impliquer dans votre démarche (par exemple via un PV d'approbation ou un document signé par la direction).

3.2.2 Le résultat

Il existe différents types d'actifs essentiels au sein de toute organisation. En voici une liste non exhaustive à titre d'exemple:

- Les **actifs primaires**, à savoir:
  - L'information, les services, les processus clés, les personnes clé,
- Les **actifs secondaires** comme:
  - Les systèmes IT supportant les actifs primaires

N'essayez pas d'avoir une liste exhaustive, concentrez-vous sur l'essentiel. Il est préférable de démarrer le processus avec uniquement un nombre limité d'actifs

que d'essayer de les lister tous. Vous risquez en effet grandement que la liste soit obsolète lorsque vous aurez terminé l'exercice.

Ce qui est important, c'est de démarrer le processus, de l'améliorer continuellement au fur et à mesure.

La Méthode Optimisée d'analyse des risques Cases (Monarc)[1] propose une approche d'identification des actifs. L'on retrouve aussi une approche encore plus détaillée dans la norme ISO 27005.

3.3 L'analyse de risques

3.3.1 L'analyse de risques en 6 points

Pour chaque actif essentiel, il est important d'effectuer une analyse de risques. Il est à noter que la section 3 du RGPD de l'Union européenne explicite la nécessité de réaliser une analyse de risques pour tout traitement de données à caractère personnel à risque.

3.3.1.1 Établissez le contexte de votre organisation

- Profil de risque (facteurs interne & externe)
  - Quel est le contexte spécifique de votre organisation/secteur spécifique ?
  - Propriétés de l'organisation?
  - Les components internes ou externes lesquels influencent le risque?
- Appétit de risque (choix de l'organisation)
  - Quel est le niveau de risque acceptable pour votre organisation ?

3.3.1.2 Modélisation du contexte

a) Identification des actifs essentiels
   - Rassembler les informations comme par exemple le flux du processus, les infrastructures, les bases de données, les brevets, les personnes clés, …
   - Rassembler les contrats avec les parties tierces (fournisseurs, sous-traitants, IT provider, cloud, etc., toute partie externe qui gère pour votre organisation des infrastructures, applications ou bases de données).

b) Identification des risques, vulnérabilités, menaces, …
   - Identifier les risques possibles au niveau de la confidentialité, l'intégrité, la disponibilité, la traçabilité, la non-répudiation et l'authenticité des données.
   - On décrit généralement la notion de "risque" comme la possibilité ("probabilité") qu'une menace déterminée/donnée (profitant d'une vulnérabilité) se présente, avec pour conséquence un impact déterminé ("gravité").

[1] http://monarc.lu/

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

- Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance.
- Processus de comparaison des résultats de l'analyse du risque avec les critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou non.

3.3.1.3 Évaluation et traitements des risques

a) Identifier les mesures de sécurité organisationnelles, opérationnelles et techniques déjà en place pour sécuriser l'actif en question.
b) Identifier les mesures de sécurité organisationnelles, opérationnelles et techniques supplémentaires pour renforcer la sécurité.
c) Évaluer le niveau de risque résiduel. Est-il à un niveau acceptable pour votre organisation ?

En matière de gestion des risques, on peut opérer une distinction entre le risque "inhérent" et le risque "résiduel".

Le risque "inhérent" renvoie à la probabilité qu'un impact négatif se produise lorsqu'aucune mesure de protection n'est prise.

Le risque "résiduel" renvoie, au contraire, à la probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent).

L'analyse du risque résiduel vous sera utile pour sélectionner et développer des actions/mesures à prendre, ce qui vous permettra de minimiser le risque résiduel.

3.3.1.4 Implémentation des mesures

L'implémentation des mesures peut inclure (selon le principe de "PPT"):

1. Les personnes ("People")
2. Les processus et procédures ("Processes")
3. La technologie ou l'infrastructure technique ("Technology or Systems")

3.3.1.5 Monitoring: évaluer l'implémentation des mesures & leurs effets sur la diminution des risques

Il n'est pas suffisant d'implémenter des mesures ; il est nécessaire de les évaluer régulièrement.

3.3.1.6 Enrichir l'analyse de risques avec des nouveaux actifs (itérer le point 1)

Votre analyse de risques est un élément dynamique qu'il faudra continuellement mettre à jour au vu des incidents, des modifications du traitement, de la maintenance de l'outil, de la modification des actifs essentiels, de l'adaptation règlementaire ou légale, ou de la disponibilité des ressources, des personnes, du temps ou du budget.

3.3.2 Quelle méthode à utiliser ?

La Méthode Optimisée d'analyse des risques Cases ("Monarc") propose une approche d'analyse de risques. L'on retrouve aussi une approche plus détaillée dans la norme ISO 27005.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Votre analyse de risques peut être très simple, comme elle peut être très détaillée…

Tout dépend de la taille de votre organisation, de la complexité des projets et de la sensibilité des données que vous traitez.

Ne sous-estimez pas le travail car, même si un projet paraît simple, les risques y afférents peuvent être importants. Il n'y a donc pas de proportionnalité entre la taille du projet et les risques liés à ce projet. Afin de vérifier l'exactitude et l'exhaustivité de votre analyse de risques, demandez à différentes personnes de votre organisation de la vérifier.

En règle générale, toute organisation est libre de choisir la méthodologie qu'elle souhaite utiliser.

Toutefois, l'utilisation d'une méthodologie comparable par d'autres organisations offre d'importants avantages.

Le résultat de votre analyse de risques sera à la base de votre plan de sécurité. Pour ce faire, vous devrez fixer en priorité les mesures de sécurité à mettre en place afin d'obtenir un plan d'implémentation à faire valider par la direction.

3.3.3 L'analyse de risques dans l'approche gestion de projets

La sécurité doit être pensée à chaque étape de tout processus de développement de votre projet. Veillez à adapter votre politique de gestion de projets au niveau de la gestion de projets pour y inclure l'analyse de risques et les mesures de sécurité à implémenter.

N'oubliez pas également que l'analyse de risques des systèmes TIC doit être effectuée dès le début du projet de développement d'une nouvelle solution ("security & privacy by design"). Elle revêt donc un caractère évolutif ! Ceci signifie qu'elle est sujette à des modifications en cours d'élaboration du projet.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

4 Mise en place des mesures de sécurité

Les mesures minimales de sécurité sont recommandées pour toute organisation, quelle que soit sa taille. Certaines ne seront pas applicables au vu du contexte de l'organisation. Cependant, ces normes étant créées pour l'ensemble du service public, elles sont adaptables à la taille et au contexte de votre organisation.

Afin de garder un lien avec les mesures décrites ci-après, l'ordre du standard ISO 27001 a été utilisé.

4.1 Politique de sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation doit disposer d'une politique de sécurité approuvée et soutenue par la direction.	Chaque organisation mettra en place une (des) politique(s) de sécurité de l'information, actualisée(s) et approuvée(s) par la direction.
	La direction devra être tenue au courant régulièrement de l'état des mesures mises en œuvre.

4.2 Organisation de la sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation mettra en place un système de gestion des risques.	Un processus de gestion des risques sera documenté, approuvé et revu périodiquement.
	Un registre des actifs et des risques y afférents ainsi que des mesures prises (réduction, acceptation, transfert) sera tenu à jour.
Chaque organisation veillera à encadrer les relations avec les fournisseurs et les autorités.	Les contrats/documents doivent clairement fixer la répartition des obligations à respecter ainsi que les responsabilités des différentes parties.
La sécurité de l'information sera intégrée dans la gestion des projets ("security by design") afin d'intégrer le plus tôt possible les aspects de sécurité.	Un processus documenté de gestion des risques de sécurité de l'information sera mis à jour et l'on veillera à sa mise en application.
Afin de mettre à jour les connaissances et de favoriser les échanges sur les dernières tendances en matière de sécurité de l'information, il sera nécessaire de participer aux forums spécialisés abordant les questions de sécurité de l'information.	Une veille technique des forums spécialisés en sécurité de l'information sera implémentée.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Mesure de sécurité	Mesures minimales à mettre en place
Afin que ces mesures organisationnelles soient appliquées, chaque organisation (in)formera son personnel et les tiers opérant sous sa responsabilité.	Un plan de formation au risque de sécurité sera développé, maintenu à jour et suivi.
	Une formation permanente du personnel et des tiers sur sa politique de sécurité et de protection des données, ainsi qu'une procédure de sanctions pour non-respect seront implémentées.
Chaque organisation veillera à désigner et mandater un responsable de la sécurité.	Un responsable en sécurité de l'information avec un mandat clair sera désigné.
	Un délégué à la protection des données avec un mandat clair sera désigné.
Chaque organisation disposera d'un tableau de bord permettant de mesurer son niveau de sécurité par rapport aux objectifs fixés par la stratégie de l'organisation.	Un tableau de bord revu, présenté à la direction et permettant d'évaluer l'état de la sécurité de l'organisation sera mis en œuvre.
Un code de conduite et de bonnes pratiques en matière d'utilisation des systèmes d'information sera élaboré, approuvé et communiqué.	Mettre en place un code de conduite pour tout utilisateur lors de la sélection, la gestion et le désengagement de vos employés, et assurément pour ceux qui ont accès à des données sensibles ou à des systèmes critiques.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Mesure de sécurité	Mesures minimales à mettre en place
	Ce code de conduite devra comporter les éléments suivants: ▪ Gestion des accès/autorisations ▪ Révocation des droits ▪ Confidentialité des données ▪ Systèmes d'accès physique aux bâtiments & infrastructures ▪ Systèmes d'accès & confidentialité des données d'accès ▪ Procédures pour définir l'utilisation correcte des outils de travail mis à disposition (mobile devices, télétravail, data catégorisation,…) ▪ Les mesures mises en œuvre pour le contrôle des opérations (Accès, stockage destruction, accès à distance, logging)
	Il est important de communiquer le code de conduite et de le rappeler régulièrement (campagnes de sensibilisation).
Un plan d'information & de formation sera adopté.	Le plan devra inclure les relations avec des tiers et les autorités.
	Une culture de sécurité intégrant la sécurité dans les processus de développement sera définie et promue.
Chaque organisation définira les règles et mesures de sécurité d'usage des supports média amovibles.	Une procédure d'utilisation des outils mobiles sera adoptée.
Une politique d'accès, de gestion des informations à distance (télétravail) sera adoptée.	Une procédure d'accès, de gestion des informations à distance (télétravail) sera adoptée.
Chaque organisation doit identifier les rôles et responsabilités des différents acteurs dans la sécurité de l'information.	Une identification des rôles et responsabilités de chacun quant à la protection de l'information ainsi que la structure de l'organisation sont des outils indispensables afin de permettre une évaluation des tâches et activités nécessaires à la mise en place de ce plan (définition d'une matrice RACI p.ex.).

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

4.3 La sécurité des ressources humaines

Mesure de sécurité	Mesures minimales à mettre en place
Une politique relative à la gestion des collaborateurs (internes et/ou externes) sera adoptée.	Des procédures couvrant les aspects suivants seront développées: Avant l'emploi: ▪ Procédures d'engagement et mesures y afférents Pendant l'emploi: ▪ Tous les collaborateurs internes et externes doivent adhérer au code de conduite de l'organisation. La résiliation ou la modification de l'emploi: ▪ Les responsabilités et les obligations relatives à la sécurité de l'information demeurent après la résiliation ou le changement d'emploi et ces termes doivent être clairement communiqués et intégrés dans le processus de gestion des collaborateurs (internes ou externes).

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

4.4 Sensibilisation, formation et développement & Communication sur la sécurité de l'information

Mesure de sécurité	Mesures minimales à mettre en place
Un plan de formation, de développement et de communication sera défini afin que tous les collaborateurs de l'organisation, internes et externes, suivent, dans la mesure du possible, la formation en matière de sécurité de l'information et soient régulièrement informés sur les adaptations apportées aux directives et procédures.	Des procédures seront élaborées pour les aspects suivants: ▪ Un programme visant à sensibiliser les employés à la sécurité de l'information, tant en interne qu'en externe ; ▪ Le programme doit être organisé à intervalles réguliers (de préférence 1 ou 2 fois par an ou plus) de sorte que les nouveaux employés soient également intégrés au programme à temps ; ▪ Cette information doit toujours être accessible aux employés de façon simple et harmonieuse ; ▪ .Les employés doivent pouvoir signaler d'éventuels incidents de sécurité sans être punis ou sans s'exposer à des actions de vengeance de la part d'autres employés ou de supérieurs hiérarchiques.
Un plan de communication sera défini pour que toutes les parties intéressées de l'organisation, en interne et en externe, reçoivent les informations nécessaires sur la sécurité de l'information, le cas échéant, et soient régulièrement informées des adaptations apportées aux lignes directrices et aux procédures.	Des procédures seront développées pour les aspects suivants: ▪ Identification des parties impliquées et mode de communication adéquat ▪ Prévoir de régulièrement tenir au courant les parties des adaptations apportées aux directives et procédures

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

4.5 La gestion des actifs

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation établira un inventaire de ses actifs essentiels, quelle que soit sa catégorie (information, données, transmission, application, réseaux, processus, systèmes, …).	Chaque élément de l'architecture sera détaillé dès la conception ("by design") et tous les éléments seront repris afin de bénéficier d'une cartographie de l'infrastructure de l'information de l'organisation ("by default").
	Chaque élément de cet inventaire sera assigné à un responsable (avec son backup) dont les données de contact seront tenues à jour.
	Pour chaque élément d'actif, les accès et autorisations accordés seront repris. Les accès et autorisations seront octroyés en tenant compte du principe "need-to-know/need-to-use".
	Lorsque le responsable est une personne extérieure à la société (fournisseur de logiciel, sous-traitant), les références du contrat seront reprises dans l'inventaire ainsi que les données de contact en cas d'urgence.
	Cet inventaire sera sécurisé mais connu des personnes clés de l'organisation et de celles devant gérer un incident.
Un inventaire des systèmes d'information sera tenu à jour.	Un inventaire des systèmes installés et des services clients (par exemple: liste des applications et utilisateurs des applications/données sur le serveur)
	L'inventaire de l'interdépendance entre les systèmes au niveau technique et fonctionnel sera tenu à jour.
	La désignation du (des) responsable(s) du système ainsi que les données de contact (personnel interne, fournisseur ou sous-traitant) sera tenu à jour.
	La configuration des systèmes
	Les procédures de backup, de restauration et d'archivage des systèmes seront tenues à jour.
	L'inventaire de la connectivité et la redondance

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Mesure de sécurité	Mesures minimales à mettre en place
	Les procédures de mise en production, changements, mises à jour et maintenance des systèmes: versioning, change & processus maintenance & mésures de sécurité.
	Les procédures de login & monitoring des systèmes
	Procédures pour destruction/décommissionnement d'un actif essentiel
	Pour chaque élément de l'infrastructure, les moyens de protection seront détaillés et assignés à un responsable déterminé. Attention de bien distinguer les personnes ayant une responsabilité opérationnelle de celles qui sont responsables au niveau du développement et du test.
Chaque organisation veillera à mettre en place une procédure de gestion des actifs de l'information en tenant compte de l'importance des données de l'organisation:	Une catégorisation des informations qui tient au minimum compte de la confidentialité, de l'intégrité, de la disponibilité et de l'authenticité requises pour cette information sera adoptée.
	Une procédure de marquage de cette information sera adoptée.
	Une procédure de manipulation de supports amovibles sera adoptée.
	Une procédure de diffusion, de stockage, d'archivage et de destruction (data life cycle management) sera adoptée.
Chaque organisation définira une politique en accord avec les obligations prescrites dans les lois et règlements en ce qui concerne les données à caractère personnel, comme le prévoit le RGPD.	Une procédure sera adaptée en tenant compte des obligations découlant du RGPD (ex: Registre des traitements art. 30 EU RGPD) ou des recommandations de l'Autorité de la protection des données.
Chaque organisation mettra en place les mesures de sécurité des données sensibles et des systèmes d'information.	Des mesures de sécurité seront adoptées pour les systèmes en fonction de la catégorisation des données.
	Définition des règles/moyens de confidentialité, intégrité et disponibilité des données et des systèmes d'information

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation mettra en place les mesures de sécurité régissant les moyens de communication électronique.	Des mesures de sécurité concernant l'utilisation des moyens de communication électroniques seront adoptées.

4.6 Le contrôle d'accès

Mesure de sécurité	Mesures minimales à mettre en place
L'organisation définira par actif (au sens large du terme) les règles claires d'accès.	De manière générale pour l'accès aux actifs essentiels, un identifiant partagé ne sera pas autorisé.
	Les niveaux d'authentification utilisés par l'organisation seront établis en adéquation avec la catégorisation de l'information déterminée dans l'analyse de risques.
Un registre des autorisations d'accès sera tenu et mis à jour par l'organisation.	Ce registre sera régulièrement revu et mis à jour.
	Ce registre permettra une administration correcte des droits d'accès, leur suivi et leur mise à jour.
	Il sera nécessaire qu'un responsable délivre une autorisation sur la base de ces différents critères (à définir par l'organisation: accréditation service, contrat)
Les utilisateurs seront clairement formés et informés de leurs devoirs & responsabilités.	Une attention particulière sera accordée à la formation et l'information sur les moyens d'accès, et notamment les mots de passe. (Reprendre les éléments pour un mot de passe fort, non partagé, ne pas écrire le mot de passe, ne pas utiliser un même mot de passe pour des usages pro & privés, …)
Pour chaque élément de l'inventaire (renforcement des mesures de sécurité, rapport à une autorité)	Les actions seront monitorées au moyen de log, dont l'accès sera sécurisé et uniquement accessible aux personnes identifiées par la direction.
	Tout acte suspect ou tout incident sera rapporté et investigué, et un journal de bord des investigations sera tenu afin de déterminer si des actions subséquentes sont nécessaires.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Mesure de sécurité	Mesures minimales à mettre en place
	Un système de détection des accès non autorisés sera tenu.
Quelques cas particuliers:	Les éléments de communication du réseau seront parties prenantes de cet inventaire et considérés comme des éléments critiques de l'architecture de l'information.
	Un élément supplémentaire sera apporté à la connectivité: afin d'assurer la continuité des opérations de l'organisation, la connectivité sera doublée.

4.7 La cryptographie

Mesure de sécurité	Mesures minimales à mettre en place
Si des mesures cryptographiques sont mises en œuvre, l'organisation détaillera:	
En règle générale, l'accès aux actifs essentiels doit être basé sur des accès individuels. Le partage de codes d'accès n'est pas permis.	Une mesure de sécurité concernant l'utilisation de la cryptographie doit être mise en place, validée, communiquée et maintenue.
Key management	Une procédure documentée concernant la gestion, l'utilisation, la protection et la durée de vie des clés cryptographiques doit être mise en place.

4.8 La sécurité physique et environnementale

Mesure de sécurité	Mesures minimales à mettre en place
Espaces sécurisés	Toute organisation doit exclusivement limiter l'accès aux bâtiments et locaux aux personnes autorisées et effectuer un contrôle à ce sujet tant pendant qu'en dehors des heures de travail.
Protection des appareils	Toute organisation doit prendre des mesures de prévention contre la perte, l'endommagement, le vol ou la compromission des actifs de l'organisation et contre l'interruption des activités de l'organisation.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

4.9 La sécurité liée aux opérations

Mesure de sécurité	Mesures minimales à mettre en place
Pour chaque élément d'actif	Login & monitoring avec rapportage des incidents et des mesures de sécurité prises
Un inventaire de l'environnement de test sera dressé.	L'environnement de test sera clairement dissocié de l'environnement de production. Il détaillera: ▪ Les autorisations ▪ Les logs ▪ Le scénario "fall back" pour updates et change ▪ Les tests & updates effectués avec timing & log
Les mesures techniques mises en place pour l'architecture seront au minimum:	▪ Antimalware/antivirus mis à jour ▪ Système de détection des intrusions ou des accès non autorisés/software non autorisés ▪ Procédures de blocage/isolement pour anomalies/accès non autorisé, … ▪ Up to date hardware & software avec test préalable des nouvelles releases & fall back scénario ▪ Gestion des incidents (y compris la communication) ▪ Avoir des procédures de backup: création, test de restauration ▪ Avoir une procédure liée au cryptage des données

4.10 La sécurité des communications

Mesure de sécurité	Mesures minimales à mettre en place
Une mesure de sécurité doit prendre en compte la sécurité des transmissions de l'information afin d'éviter les accès non autorisés aux infrastructures et aux données de l'organisation, que cet accès soit volontaire ou non.	Avoir un système détaillé et maintenu, revu, des contrôles d'accès tant physiques que logiques
Cette mesure de sécurité devra tenir compte de l'accessibilité requise pour les systèmes de l'organisation.	Mettre en place un inventaire des flux, de leurs responsables et des accès octroyés

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

4.11 Acquisition, développement et maintenance des systèmes d'information

Mesure de sécurité	Mesures minimales à mettre en place
Implémentez des contrôles pour l'acquisition, le développement et la maintenance de tout nouveau système. L'aspect d'outsourcing, l'utilisation de services en nuage ou l'achat de produits nécessitent une attention particulière.	Une approche structurée placée sous la supervision d'un responsable de l'organisation devra être développée afin de gérer efficacement l'intégration, le développement, la maintenance et le décommissionnement des solutions choisies par l'organisation. Un inventaire des systèmes choisis ainsi que la référence aux contrats et obligations (SLA, NDA) sera établi par l'organisation afin d'assurer le suivi et la gestion des solutions externalisées.
De plus, chaque organisation tiendra un journal avec les différents éléments suivants:	▪ Les changements ▪ Les incidents & leurs conséquences ▪ Les accès ▪ La maintenance ▪ Les mesures de sécurité mises en place
Le journal spécifiera aussi les mesures de sécurité mises en place pour:	▪ Les mesures de continuité ▪ L'intégrité des données ▪ Le problème de confidentialité ▪ La disponibilité des systèmes ▪ Les mesures pour la gestion des incidents
L'organisation mettra en œuvre des procédures afin de maintenir ses solutions à jour et assurera une mesure de sécurité de backup testée tant pour ses systèmes que pour ses données.	

4.12 Relations avec les fournisseurs

Mesure de sécurité	Mesures minimales à mettre en place
L'organisation s'assurera que les contrats entre parties mentionneront les mesures de sécurité imposées par l'organisation, les lois et règlements (notamment le RGPD) ainsi que les éléments de contrôle et de revue.	
Chaque organisation veillera à faire appel aux services de cloud computing qui correspondent aux	Basé sur une analyse des risques pour les services / données externalisées – pour ce faire, vous pouvez

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Mesure de sécurité	Mesures minimales à mettre en place
mesures de sécurité nécessaires pour l'organisation.	utiliser les rapports d'audit disponibles (ISO, ISAE3402, ENISA, SANS, CSA, etc.). Valider les rapports d'audit et les certifications des fournisseurs de services cloud

4.13 Politique Coordonnée pour publication des vulnérabilités de sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Une Politique Coordonnée pour publication des vulnérabilités (*Coordinated Vulnerability Disclosure Policy* – ci-dessous CVDP) **L'organisation élabore et applique une CVDP.**	La politique doit être approuvée légalement par un responsable de l'entreprise (p.ex. le directeur). Une CVDP est un ensemble de règles établies préalablement par une organisation qui est responsable du traitement de l'information. Cette politique permet aux chercheurs en sécurité (ethical hackers) ou au grand public de chercher des vulnérabilités dans les systèmes de l'organisation et de les signaler de façon coordonnée à l'organisation.
	Le contenu de la CVDP doit être **disponible** et **accessible sur le site web public**. Le contenu doit, dans la mesure du possible, être disponible dans différentes langues. On envisage de rédiger un texte consolidé mais complet qui renvoie clairement vers: ▪ **L'applicabilité de la politique** ; ▪ Les limites de droit d'accès ; ▪ La manière dont un ethical hacker **peut changer ou détruire, ou non, des données**.

4.14 Gestion des incidents liés à la sécurité de l'information

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation mettra en place un plan de gestion des incidents qui reprendra:	Determiner les rôles et responsabilités
	Les outils de détection (internes ou externes)

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

Mesure de sécurité	Mesures minimales à mettre en place
	La notification par tout employé ou partie tierce d'intrusion, d'élément suspicieux, de perte ou de destruction
	Les niveaux d'alerte – définition des critères d'escalation vers une crise
	La procédure de gestion de crise (y compris la communication)
	L'information et la formation sont nécessaires par le biais de différents canaux.
	Liés aux données à caractère personnel en suivant les prescrits du RGPD art. 33.5 RGPD de l'UE
	Dans le respect de toute autre obligation règlementaire et/ou sectorielle (par exemple énergie, banque, télécom)
Chaque incident sera analysé afin d'évaluer la pertinence de nouvelles mesures de sécurité.	Les "lessons learned" (enseignements tirés) de chaque incident (interne et/ou externe) permettront d'améliorer la procédure de gestion des incidents pour l'organisation.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

4.15 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Mesure de sécurité	Mesures minimales à mettre en place
Pour tout système critique ou toute donnée sensible nécessaires à la continuité de l'organisation, un plan de continuité sera mis en place.	Une attention particulière sera portée aux points suivants: • Inventaire des systèmes/actifs critiques • Gestion des risques • La compétence des employés responsables des différents processus/actifs essentiels à l'organisation • Les niveaux requis de criticité pour l'activation du plan de continuité • La priorisation des actifs essentiels dans leur restauration • La gestion de la communication
Maintenance du plan de continuité	Une révision et adaptation de ce plan de continuité sont nécessaires, à l'instar d'un test/d'une simulation.

4.16 Encadrer les relations avec les tiers et les autorités

Mesure de sécurité	Mesures minimales à mettre en place
Conformité aux dispositions légales et règlementaires	Chaque organisation agira conformément aux dispositions légales et règlements.

4.17 Evaluation des mesures des sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation organisera régulièrement:	Une évaluation interne ou externe sur la sécurité de l'information. Cette évaluation externe pourra être réalisée par le service Fédéral d'Audit Interne (FAI).
	Un rapport de contrôle sur la situation de la sécurité rédigé par un auditeur interne ou le CISO qui sera présenté au comité de direction

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

5 Revue annuelle du plan de sécurité avec l'approbation de la direction

Il est conseillé de revoir ce plan de sécurité annuellement avec la direction. Cela permettra de le corriger, de compléter le plan de la sécurité de l'information ainsi qu'à la protection des données.

Le plan de sécurité de l'information est amené à évoluer dans le temps. Il pourra notamment être revu afin de prendre en compte:

- Les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- Les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'audits ;
- Les évolutions des contextes organisationnels, juridiques, réglementaires et technologiques.

Le suivi de ces évolutions est assuré par la direction des différents SPF qui a pour principales missions:

- De suivre la mise en œuvre des plans de sécurité ;
- De mesurer les progrès et l'état de la sécurité de votre organisation ;
- De proposer des mises à jour ;
- De proposer des documents complémentaires et des directives permettant d'en faciliter ou d'en préciser la mise en œuvre ;
- De suivre les évolutions des documents techniques.

Certaines organisations sont obligées de faire rapport sur l'état d'avancement de leur plan de sécurité.

CENTRE FOR

CYBER SECURITY BELGIUM

Rue de la Loi, 16 – Brussels

6 Panel d'experts

Ce document a été élaboré grâce à la participation active des conseillers en sécurité et experts issus des instances suivantes:

Instance
SPF Justice
DGCC
Police Fédérale
SPF Chancellerie
SPF Santé
SPF Economie
CCB
SPF BOSA

CENTRE FOR

CYBER SECURITY BELGIUM

Rue de la Loi, 16 – Brussels

7 Acronymes & Abréviations

7.1 Terminologie

Acronyme	Description
Les techniciens de l'information	peuvent être définis comme toutes les personnes qui possèdent, dans le cadre de leurs responsabilités pour un système TIC, des droits d'accès qui excèdent l'usage fonctionnel des données. Il s'agit entre autres des développeurs, des gestionnaires et opérateurs systèmes, des gestionnaires de données, des développeurs et gestionnaires de logiciels, des opérateurs de réseau, des consultants et des sous-traitants.
Le conseiller en sécurité de l'information	soutenu par le responsable de traitement promeut le respect des lois et règlements en matière de sécurité informatique. Il a une mission d'avis, de stimulation, de documentation, de contrôle et de promotion du respect des règles de sécurité imposées par une disposition légale ou règlementaire ou en vertu d'une telle disposition. Il promeut l'adoption, par les personnes employées dans l'organisation, d'un comportement favorisant la sécurité. Dans ce cadre, il est à l'évidence un partenaire privilégié de beaucoup de personnes dans l'organisation comme par exemple des gestionnaires d'information, des "data owner", des "business owners", mais aussi de beaucoup de partenaires externes, des fournisseurs, des autorités, …
Le responsable du traitement	désigne le responsable de tout traitement des informations.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

7.2 Acronymes

Acronyme	Description
CIA	Confidentialité, intégrité et disponibilité *Confidentiality, integrity and availability (EN)*
CVDP	Politique coordonnée pour publication des vulnérabilités (PCPV, FR) *Coordinated Vulnerability Disclosure Policy* (EN)
PCPV	Politique coordonnée pour publication des vulnérabilités
DGCC	Direction Générale Centre de Crise
PCA	Plan de continuité des activités
PDCA	Plan, Do, Check, Act (EN)
RGPD	Règlement Général sur la Protection des Données General Data Protection Regulation, GDPR (EN)

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

CENTRE FOR
CYBER SECURITY
BELGIUM

CENTRE FOR

CYBER SECURITY BELGIUM

Rue de la Loi, 16 – Brussels

CHANCELLERY OF
THE PRIME MINISTER

.be

CENTRE FOR
CYBER SECURITY
BELGIUM

Les informations fournies :

- sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières ;
- ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points ;

Editeur responsable :

CENTRE POUR LA CYBERSECURITE BELGIQUE

Rue de la Loi, 16

1000 Bruxelles

CENTRE FOR

CYBER SECURITY BELGIUM

Rue de la Loi, 16 – Brussels

CHANCELLERY OF
THE PRIME MINISTER

.be