Federal Information Security Policy Guideline

Guide pour la catégorisation des informations

21/11/2019

FISPDOC01 V1.3

Remarque importante : Le présent document est un guide qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures présentées sont considérées comme des mesures minimales applicables raisonnablement de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales et des bonnes pratiques en matière de sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont requises pour un service fédéral pour des raisons réglementaires ou autres raisons formelles et impérieuses, on peut supposer que ces mesures sont prioritaires sur les mesures prévues dans le présent guide.

FISP

Groupe de travail

.be

Table des matières

Contenu du présent document

Orientation du document

Le présent document fait partie intégrante de la méthodologie pour la sécurité de l'information au sein de l'Administration fédérale (projet FISP).

Objectif de sécurité du document

Les résultats de la catégorisation de l'information sont une contribution importante aux différents processus qui font partie de la gestion de la sécurisation de l'information (par ex. la gestion des risques de l'information, le choix du fournisseur de services pour les solutions 'cloud', le développement du plan d'action pour la sécurité de l'information,...).

Champ d'application

La politique de 'catégorisation de l'information' s'applique à toutes les informations légalement non classifiées qui sont consultées, traitées, enregistrées ou publiées par l'administration fédérale (et ses prestataires de service). Toutes les informations qui sont classifiées selon la loi du 11/12/1998 relèvent d'une autre réglementation spécifique et de la responsabilité de l'Autorité Nationale de Sécurité.

Il s'agit à la fois de l'information qui est créée par l'organisation même ou qui provient d'autres autorités, citoyens, entreprises, partenaires et tiers, ou qui leur est destinée.

Concrètement, il s'agit des éléments suivants :

- Le traitement de l'information dont l'organisation est responsable :
  - Information des organisations au sein de l'administration fédérale.
- Les mesures relatives au traitement et à l'utilisation de l'information au sein de l'organisation
  - Information d'autres autorités, citoyens, entreprises, partenaires et tiers.

La politique de 'catégorisation de l'information' comprend uniquement l'élaboration et la maintenance du modèle de catégorisation et non son application à l'information présente dans le traitement et l'utilisation de l'information de l'administration fédérale.

Confidentialité du document

Distribution publique

Clause de non-responsabilité

Il s'agit d'une directive basée sur les pratiques internationales en matière de catégorisation de l'information. Si vous souhaitez appliquer cette directive à votre organisation, vous devez d'abord procéder à une évaluation et vérifier si d'autres restrictions, règles ou pratiques légales s'appliquent à votre organisation. Adaptez la politique de sécurité en fonction de votre organisation !

Lors du Conseil des ministres du 3 mai 2019, un avant-projet de loi a été soumis, à savoir la révision de la loi du 11/12/1998. Si cette loi est adoptée, la politique FISP sera mise à jour. La politique actuelle ne tient pas compte de futurs développements légaux.

Responsabilités

Le présent document est destiné au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de l'administration fédérale, aux responsables du traitement de l'information (y compris les sous-traitants des systèmes d'information), à l'officier de sécurité et aux autres intervenants dans des domaines connexes (ex. le gestionnaire de documents).

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Introduction

Les autorités fédérales traitent de nombreuses informations. Ces informations sont sensibles aux risques en matière de disponibilité, intégrité et confidentialité. Selon la sensibilité de l'information, celle-ci doit être protégée selon une méthodologie afin de gérer les risques. Cela permet de limiter les risques à un niveau de protection acceptable préalablement défini. Le schéma de catégorisation donne une indication simple et rapide de l'importance de l'information et constitue ainsi une base pour l'évaluation des risques.

Cette méthode de catégorisation favorise en outre la collaboration entre les différentes organisations qui traitent l'information pour l'administration fédérale, d'autres autorités, des entreprises et les citoyens. Les gestionnaires qui ne sont pas familiarisés avec le contenu et la valeur des données sont ainsi aidés dans la mise en œuvre des mesures de sécurité nécessaires.

Le présent document donne des explications sur l'importance et la manière dont les données peuvent être catégorisées. Nous avons délibérément choisi de ne pas utiliser le mot 'classification' dans tout le document afin d'éviter autant que possible toute confusion avec les données classifiées officiellement sur la base de la loi du 11/12/1998.[1]

Principe de fonctionnement

Généralités

Les organisations de l'administration fédérale devraient garantir le niveau de protection de l'information, exprimé en niveaux de catégorisation, selon un schéma de catégorisation interne conforme à la législation spécifique en la matière, ainsi qu'à la réglementation internationale.

Si les principes décrits dans la législation et la réglementation diffèrent des principes du schéma de catégorisation interne de l'organisation fédérale, la règle la plus stricte sera toujours d'application. En outre, en cas de contradiction, les principes légaux ou juridiques auront toujours la priorité par rapport aux principes du schéma de catégorisation interne.

Lors de la définition d'une catégorisation, le niveau le plus 'bas' est toujours l'objectif visé, car d'une part une catégorisation trop élevée génère automatiquement des coûts inutiles et complique les processus et d'autre part, un niveau trop élevé limite trop l'accès à l'information pour le public. Cela entraînerait naturellement des problèmes dans les processus de l'organisation.

Les composantes d'une chaîne de traitement peuvent avoir chacune un niveau de catégorisation différent, mais les mesure de sécurité applicables sont basées sur la composante ayant la classification la plus élevée.

Les mesures de contrôle doivent être adaptées aux risques, sur la base des possibilités techniques et des coûts des mesures à prendre. Cela dépend de la situation. Plus sensible est l'information, plus grand est le risque. Selon le contexte dans lequel elle est utilisée, plus lourdes seront les exigences pour la sécurité de l'information. Globalement, si les mesures permettent d'augmenter la sécurité et la confidentialité moyennant de faibles coûts supplémentaires, elles peuvent être considérées comme "appropriées". Des mesures permettant d'augmenter la sécurité et la confidentialité ne sont plus considérées comme "appropriées" lorsque les coûts de la réduction des risques sont disproportionnellement élevés. Il est indispensable que les risques et les mesures de gestion soient en équilibre.

[1] Pour plus d'information à ce sujet, voir le chapitre "Informations classifiées".

Toute organisation fédérale qui traite des informations via des systèmes d'information court certains risques car ces informations et systèmes d'information sont exposés à des menaces et des problèmes internes et externes. La réalisation d'une évaluation des risques permet d'identifier les risques pour les systèmes d'information, ainsi que leur importance. Cela détermine ensuite les mesures de sécurité qui doivent être prises pour amener les risques à un niveau acceptable. Le schéma de catégorisation interne proposé peut dès lors être considéré comme "une forme simplifiée d'évaluation des risques".

Rôles et responsabilités

Tous les schémas de catégorisation sont proposés par le conseiller en sécurité de l'information (CISO). L'équipe DPO soutiendra le CISO dans le cadre de la vérification du respect des exigences du règlement général européen en matière de protection des données. Le schéma proposé sera ensuite validé par le management de l'organisation fédérale. Le management portera dès lors aussi la responsabilité de la classification et la communiquera à tous les intéressés.

Sur la base de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, un officier de sécurité est également désigné. Cet officier de sécurité supportera tout ce qui relève de cette loi.[2]

Les rôles et responsabilités suivants ont été déterminés sur la base d'un modèle RACI classique.

	Responsable	Propositions	Support
Schéma de catégorisation	Management	Chief Information Security Officer (CISO)	Data Protection Officer

Application des lois, règlements et normes internationales

Les principes des lois, règlements et normes internationales doivent être respectés indépendamment du schéma de classification interne défini par l'institution.[3] On peut donc déroger aux règles de classification internes et aux mesures de protection qui y sont liées pour se conformer à la loi.

Pour des informations émanant d'autres pays ou d'institutions internationales établies en Belgique auxquelles a accès l'institution, l'institution doit agir "au nom de l'institution d'origine" ("propriétaire" de l'information). Dans les cas précités, l'institution doit appliquer les mesures de sécurité correspondant au niveau de classification de l'information concernée.

Catégorisation de l'information créée par l'institution

L'organisation fédérale devrait catégoriser toutes les informations (et les moyens d'information) qui ne relèvent pas de la réglementation ou de la législation relatives à la classification.

Les informations non catégorisées seront considérées comme "catégorie 1" de sorte que ces informations peuvent circuler librement dans l'entreprise et ne peuvent être communiquées au public ou à des tiers qu'en respectant un processus d'approbation et de communication. Ces informations peuvent être communiquées à

[2] Pour plus d'information à ce sujet, voir le chapitre “Informations classifiées".

[3] Notamment le RGPD, la loi du 11/12/1998, ...

des contractants ou à des partenaires si elles sont importantes pour l'exécution d'une mission et si leur protection peut être garantie.

La catégorisation reflétera l'importance de l'information pour l'entreprise en termes de valeur pour l'institution, de criticité, de sensibilité (confidentialité, intégrité, disponibilité) et d'exigences réglementaires, légales et contractuelles. L'information doit par conséquent être catégorisée de manière à bénéficier d'une protection suffisante au sein de l'institution durant toute sa durée de vie. Il sera nécessaire d'associer une obligation de secret à toutes les informations, sauf celles relevant de la "catégorie 0".

Un schéma sera établi, composé de différentes catégorisations et comprenant des critères et des accords de subdivision pour le contrôle régulier de la classification. Ce schéma devra être cohérent dans toute l'institution, de manière à ce que chacun catégorise les informations de la même manière et ait les mêmes objectifs et les mêmes mesures dans le domaine de la sécurité de l'information.

La catégorisation de l'information sera réalisée par le propriétaire/détenteur de l'information ou par la personne qui gère le département responsable de l'information. Cette personne a généralement une connaissance suffisante des conséquences en cas de perte de disponibilité, d'intégrité et de confidentialité de cet actif. Le propriétaire/détenteur connaît aussi la législation et la réglementation à laquelle est soumise l'information, ainsi que les conséquences en cas de transgression.

Labellisation de l'information

Les organisations fédérales devraient établir, valider, mettre en œuvre, communiquer et maintenir des procédures et registres adéquats pour la labellisation et le traitement de l'ensemble des compilations d'information, des supports d'information et des systèmes d'information conformément au schéma de catégorisation interne. Cela comprend à la fois l'information et les moyens physiques et électroniques correspondants. Il faudrait également tenir compte de la labellisation adéquate des métadonnées (invisibles à l'œil nu). La labellisation devra refléter le schéma de catégorisation et être respectée pour toutes les informations dotées d'une catégorisation.

Manipulation des moyens d'information

Des procédures devraient être établies pour le traitement, l'enregistrement et la communication d'informations conformément à leur catégorisation. Les aspects suivants devraient être pris en considération lors de la manipulation des moyens d'information :

- restriction d'accès sur la base du niveau de catégorisation et des principes "Need to know" et "Need to have" ;
- enregistrement des destinataires autorisés des moyens d'information ;
- protection des copies temporaires ou permanentes de l'information à un niveau conforme au niveau de protection de l'information originale ;
- marquage (labellisation) de toutes les copies des moyens d'information pour le(s) destinataire(s) autorisé(s) ;
- stockage des moyens ICT conformément au niveau de catégorisation et/ou aux spécifications produit du fournisseur.

Les accords avec d'autres organisations avec lesquelles des informations sont échangées devraient comprendre des procédures pour identifier la catégorisation de l'information et interpréter les labels / niveaux de catégorisation des partenaires. Même si les appellations de la catégorisation d'un schéma de catégorisation d'une autre organisation sont identiques ou comparables à celles d'une organisation de l'administration fédérale, cela ne signifie pas que la valeur ajoutée est identique ou comparable.

Schéma de catégorisation

Le niveau de protection de l'information s'exprime en niveaux de catégorisation pour la confidentialité, l'intégrité et la disponibilité de l'information (C.I.D.).

C.I.D.

Confidentialité

ISO / CEI 27000 : “propriété selon laquelle l'information n'est pas diffusée ou communiquée aux personnes, entités ou processus non compétents"

Intégrité

ISO / CEI 27000 : “Propriété de la précision et de l'exhaustivité”

Disponibilité

ISO / CEI 27000 : “Propriété de l'accessibilité et de l'utilisabilité à la demande d'une entité autorisée"

Modèle de catégorisation

Dans le contexte de cette catégorisation, l'information sera principalement catégorisée en ce qui concerne l'aspect confidentialité, comme le montre le tableau ci-dessous. La mise en œuvre des objectifs et des mesures de sécurité tient cependant aussi compte des problèmes relatifs à l'intégrité et à la disponibilité des données.

Les niveaux de catégorisation donnent une indication rapide des sensibilités et de la situation critique de l'information et donnent un aperçu clair des niveaux de protection requis. Sur la base du niveau de protection requis, on peut déterminer quelles mesures devraient être mises en œuvre et combien. Si la catégorisation est par exemple supérieure à "1", il faut mettre en œuvre des mesures supplémentaires.

Les informations sont caractérisées par les paramètres suivants :

- le type de données : en fonction des domaines inhérents à l'organisation auxquels la donnée appartient.
- la sensibilité : détermine en général l'impact de la perte ou de la diffusion des informations.

Pour simplifier l'utilisation de l'information, chaque catégorie reçoit un code unique sous la forme d'un chiffre <N>. De plus, nous appliquons un code couleur unique pour améliorer l'identification visuelle. Les organisations fédérales peuvent enrichir les labels graphiques avec une signification spécifique au contexte.

Catégorie	
	La **catégorie « 0 »** a pour conséquence que l'information peut être diffusée sans problème. La diffusion ne porte pas atteinte aux intérêts de l'organisation de l'administration fédérale, d'un service ou du fonctionnement d'un groupe de travailleurs. **Destination** : groupes cibles externes La mention spécifique de cette catégorie sur le support d'information est nécessaire. Une exception s'applique lorsque par la nature du support de l'information, celui-ci peut être considéré comme public par tout le monde. (par ex. dépliants, sites web publics, etc.)

	Cette information peut également être diffusée via les réseaux sociaux.
	La **catégorie « 1 »** est attribuée lorsqu'un usage inadéquat de l'information : • a une probable influence sur l'intérêt d'un service ou est susceptible de compromettre le fonctionnement d'un travailleur ou d'un groupe de personnes dans le cadre de leur fonction au sein de l'organisation ; • a un impact sur les droits à la vie privée d'un groupe restreint (exprimé en pourcentage) ou de personnes individuelles. Toutes les informations utilisées et diffusées au sein des organisations de l'administration fédérale, qui ne sont pas marquées par une autre catégorie, sont automatiquement considérées comme relevant de la catégorie 1. **Destination** : groupes cibles internes composés de travailleurs internes, externes (par contrat), temporaires, ... Ces informations ne peuvent être échangées avec des parties externes que s'il s'agit de partenaires connus et uniquement si elles sont nécessaires pour un projet et/ou un partenariat. La signature d'une déclaration de confidentialité (NDA) est également nécessaire. Durant l'échange d'informations de "Catégorie 1" en dehors de l'organisation, le niveau de catégorisation doit être clairement marqué visuellement. Il va de soi que l'information ne peut pas être diffusée via les réseaux sociaux.
	La **catégorie « 2 »** est attribuée lorsqu'un usage inadéquat des informations (par exemple en raison d'une protection insuffisante des données) : • nuit à l'un des intérêts de l'organisation fédérale ou compromet le fonctionnement du service ; • a une influence sur les droits à la vie privée d'un groupe de personnes ou de personnes vulnérables et/ou d'enfants. **Destination** : l'information est réservée à un groupe restreint de collaborateurs de l'organisation de l'administration fédérale ou à des partenaires bien déterminés. Si nécessaire, cette information peut être échangée pour l'exécution des tâches et de la mission. L'échange avec des partenaires sur la base du même principe nécessite l'approbation du management (niveau supérieur) et seulement après, la signature d'une déclaration de confidentialité (NDA). La labellisation de l'information est indispensable à tout moment. Pendant l'échange d'information (par ex. des e-mails) de "catégorie 2", il y a lieu également de préciser clairement à qui cette information est destinée (par ex. TLP). Et ce, afin que l'information puisse continuer à se voir appliquer les mesures de sécurité adéquates.
	La **catégorie « 3 »** est attribuée lorsqu'un usage inadéquat des informations : • peut nuire gravement aux intérêts essentiels des organisations fédérales ;

	• a un impact sur le droit à la vie privée d'un groupe de personnes ou de personnes vulnérables et/ou d'enfants.[4] Les données sont catégorisées "3" lorsque la publication, la modification ou la destruction non autorisée de ces données peut donner lieu à un niveau de risque considérable pour les organisations fédérales. Comme exemples de données de catégorie 3, citons les données qui sont protégées par la réglementation fédérale ou européenne en matière de confidentialité et les données qui sont protégées par des accords de confidentialité. Le niveau le plus élevé des contrôles de sécurité doit être appliqué à ces données spécifiques. **Destination :** Ces informations doivent être protégées contre l'accès illicite. Toutes les informations sont réservées à un groupe restreint de collaborateurs des organisations fédérales ou à des partenaires bien déterminés. Les données de catégorie 3 sont des "déclencheurs d'alerte", c'est-à-dire qu'il y a une notification automatique d'accès non autorisé aux personnes concernées. Ces informations ne peuvent être échangées que par les personnes qui sont dûment identifiées par le propriétaire des données et lorsque cela est strictement nécessaire pour l'exécution des tâches et de la mission (doit être connue). L'échange avec des partenaires selon le même principe nécessite l'approbation, en plus de la destination, (niveau supérieur) du propriétaire des données et seulement après, la signature d'une obligation de confidentialité (NDA). La labellisation de l'information est indispensable à tout moment. Pendant l'échange d'information (par ex. des e-mails) de “catégorie 3”, il y a lieu également de préciser clairement à qui cette information est destinée (par ex. TLP). Et ce, afin que l'information puisse continuer à se voir appliquer les mesures de sécurité adéquates. Le propriétaire du document doit mentionner le groupe cible de cette information dans le document. Toute publication de ce type d'information peut être considérée comme un écart de conduite grave.
	La **catégorie « 4 »** concerne les données classifiées sur la base de la loi du 11/12/1998.[5] Il s'agit des données, du matériel, des technologies, ... dont la connaissance ou l'utilisation est susceptible de compromettre sérieusement le fonctionnement de la Belgique, des institutions internationales ou des accords bilatéraux / multilatéraux / internationaux. Par souci de cohérence réglementaire et législative, tant au niveau national qu'au niveau européen, ce niveau de catégorisation s'applique aux organisations fédérales. Les mesures de sécurité à appliquer aux données doivent satisfaire aux objectifs et aux mesures imposés par les instances chargées de la qualification juridique. Les données de catégorie 4 sont des "déclencheurs d'alerte", c'est-à-dire qu'il y a une notification automatique d'erreur d'accès aux personnes et institutions concernées.

[4] Art. 10 et 9 du RGPD

[5] Pour plus d'information à ce sujet, voir le chapitre “Informations classifiées".

Informations classifiées (Loi du 11/12/1998)[6]

La “classification” est le processus par lequel on attribue à des informations, documents, données, matériels ou matières, sous quelque forme que ce soit, un niveau de protection donné en vertu de la loi ou des conventions ou traités qui engagent la Belgique, principalement concernant les intérêts nationaux et internationaux suivants :

- Sauvegarde de l'intégrité du territoire national et des plans de défense militaire ;
- Sûreté extérieure de l'État & relations internationales de la Belgique ;
- Potentiel économique et scientifique de la Belgique ;
- Sécurité des ressortissants belges à l'étranger.

La "Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité" (ci-après dénommée "Loi du 11/12/1998") définit les critères de classification, ainsi que les compétences et responsabilités des fonctionnaires habilités à utiliser ces données. Un niveau de classification est attribué sur la base du contenu, jamais selon les nature du destinataire ou de l'urgence. Seule l'autorité d'origine est compétente pour classifier, changer le niveau de protection et déclassifier.

Niveaux de classification

Il y a 3 niveaux de classification selon le dommage que peut entraîner une utilisation inadéquate pour les intérêts précités :

- Dommage = “**Confidentiel**”
- Dommage grave = “**Secret**”
- Dommage très grave = “**Très Secret**”

Ce marquage doit aussi être clairement visible sur chaque page des documents classifiés, avec l'inscription “Loi du 11/12/1998". Le marquage "Diffusion limitée” n'a pas de protection juridique, cela indique seulement qu'il s'agit d'informations sensibles ne pouvant pas être diffusées en dehors du groupe cible. Dans un proche avenir, une quatrième classification (plus basse) viendra s'ajouter, à savoir la catégorie "Restricted" afin de pouvoir répondre à des accords internationaux ; différents pays et organisations internationales (UE, OTAN, etc.) ont en effet une classification légale au niveau "Restricted".

Le tableau ci-dessous montre par exemple les différents niveaux de classification utilisés en Belgique, dans l'Union européenne (UE) et au sein de l'Organisation du Traité de l'Atlantique Nord (OTAN) :

Niveaux de classification				
National	Très secret	Secret	Confidentiel	(Diffusion restreinte)
OTAN	Cosmic/Focal Top Secret	NATO Secret	NATO Confidential	NATO Restricted
Europe (UE)	EU Top Secret	EU Secret	EU Confidential	EU Restricted

Les habilitations de sécurité et quelques principes de base

Une personne qui a besoin d'avoir accès à des informations classifiées doit répondre à quatre critères :

[6] Au moment où cette politique a été créée, un avant-projet de loi a été soumis au Conseil des ministres, à savoir la révision de la loi du 11/12/1998. Si cette loi est adoptée, la politique du FISP sera mise à jour. La politique actuelle ne tient pas compte de futurs développements légaux.

1. travailler pour une entreprise ou une administration qui est habilitée par l'Autorité nationale de Sécurité (ANS), ou enregistrée auprès de celle-ci, pour pouvoir traiter des informations classifiées ;
2. posséder une habilitation de sécurité pour individus au niveau requis ;
3. démontrer un "besoin d'en connaître" (le “need to know”) ;
4. avoir reçu un briefing de sécurité.

Quelques exemples d'utilisation inappropriée des informations classifiées (peines d'emprisonnement et amendes) :

- Consultation dans un espace public ;
- Communication à des personnes sans habilitation de sécurité valable ;
- Reproduction sans l'accord de l'autorité d'origine ;
- Conservation en dehors d'une zone classifiée ;
- Non-respect des conditions d'envoi et de destruction ;
- Toute forme d'utilisation violant les règles de sécurité définies par la Loi du 11/12/1998.

L'Officier de sécurité

Chaque organisation qui traite des informations classifiées doit désigner un officier de sécurité (OS), voir l'art. 13 de la Loi du 11/12/1998 : "Le membre du personnel titulaire d'une habilitation de sécurité, au sein d'une personne morale titulaire d'une habilitation de sécurité, désigné par la direction de la personne morale pour veiller à l'observation des règles de sécurité. Les officiers de sécurité relèvent, dans l'exercice de leurs missions, de l'Autorité de Sécurité".
L'officier de sécurité est responsable vis-à-vis de l'administration et intervient en tant que personne de confiance entre l'organisation, l'ANS et le service de renseignement.
Cette personne a pour principales responsabilités de :

- Veiller à l'observation des règles de sécurité au sein de la personne morale dans laquelle elle a été désignée (directives ANS).
- Tâches spécifiques imposées dans le cadre de la procédure de demande et d'octroi d'habilitations de sécurité (voir Loi du 11/12/1998).

Gestion du document

Historique

Date	*Auteur*	*Version*	*Description des modifications*
23/04/2019	BOSA	V.0.1	Première ébauche
29/04/2019	FISP workgroup	V.0.2	1e mise à jour après la réunion FISP
24/05/2019	FISP workgroup	V.1.0	2e mise à jour sur la base de remarques des participants au GT FISP
03/07/2019	FISP workgroup	V.1.2	Amélioration lisibilité
21/11/2019	FISP workgroup	V.1.3	Distribution publique

Approbations

Date	*Approbateur(s)*	*Version*
21/11/2019	FISP workgroup	V.1.3

Sources

Ce document a été rédigé à l'aide des sources suivantes :

- Classification de l'information de l'Autorité flamande
- Loi du 11/12/98 relative à la classification et aux habilitations, attestations et avis de sécurité
- Règlement (UE) 2016/679 du Parlement européen et du Conseil / 27 avril 2016 (GDPR/RGPD)
- Classification des données BCSS
- ISO/CEI 27001/2

Lien avec une autre politique

Dépendance de documents internes

Réf.	*Titre*
FISPDOC08	*Aperçu général pour la sécurité de l'information au niveau fédéral*

Positionnement de la politique par rapport à la norme ISO 27001

Section	***Objectifs et mesures de référence***	*En relation (X = Oui)*
	Contexte de l'organisation	
	Leadership	
	Planification	
	Support	
	Fonctionnement	
	Évaluation des performances	
	Amélioration	

Positionnement de la politique par rapport à la norme ISO 27002

Section	**Objectifs et mesures de référence**	En relation *(X = Oui)*	Objectifs/Mesures *(Détail)*
	Politique de sécurité de l'information		
	Organisation de la sécurité de l'information	*X*	
	Sécurité des ressources humaines		
	Gestion des actifs		
	Contrôle d'accès		
	Cryptographie		
	Sécurité physique et environnementale		
	Sécurité opérationnelle		
	Sécurité des communications		
	Acquisition, développement et maintenance des systèmes d'information		
	Relations avec les fournisseurs		
	Gestion des incidents liés à la sécurité de l'information		
	Sécurité de l'information dans la gestion de la continuité de l'activité		
	Conformité		