Federal Information Security Policy Guideline

Guide pour le contrôle et la sécurité des accès physiques

21/11/2019

FISPDOC02 V1.0

FISP Groupe de travail

.be

TABLE DES MATIÈRES

Contenu du présent document

Orientation du document

La présente directive donne un aperçu des principes majeurs liés à la sécurisation physique et à la sécurisation de l'environnement de l'organisation.

Objectif de sécurité du document

L'objectif de la présente directive est de prévoir des mesures minimales visant à sécuriser les informations contre l'accès physique non autorisé, la détérioration et la manipulation des informations, ainsi que les installations de traitement de l'information de l'organisation.

Champ d'application

Cette politique de sécurité de l'information est applicable à toutes les informations qui circulent dans les organisations fédérales.

Confidentialité du document

Distribution publique

Clause de non-responsabilité

Il s'agit d'une directive fondée sur les pratiques internationales en matière de mesures minimales de sécurisation physique dans un contexte de sécurité 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 !

Responsabilités

Chaque organisation approuve les mesures décrites, pour toutes les informations et tous les systèmes d'information dont elle a la responsabilité.

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Introduction

La sécurisation physique et la sécurisation de l'environnement impliquent des mesures visant à prévenir ou à limiter les événements physiques tels que l'accès non autorisé, la perte, le vandalisme et l'intrusion. Elle concerne également la sécurisation contre les facteurs environnementaux tels que les catastrophes naturelles, la foudre et les inondations, l'interruption de services d'utilité publique... La valeur du matériel, la sensibilité des données et la discontinuité du traitement des données sont des raisons suffisantes pour prendre les mesures de sécurisation physique souhaitées.

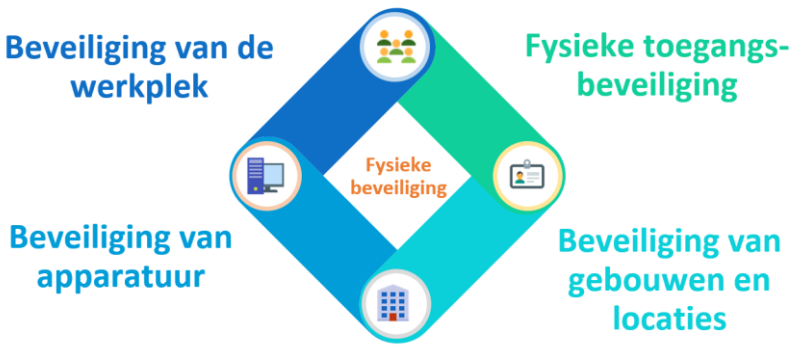
La sécurisation physique exige donc une attention particulière lors de l'aménagement des sites, des bâtiments, des salles, etc. Cette attention particulière est surtout importante pour les zones critiques, telles que les sites disposant de matériel technique, les centres de données, etc. En outre, une attention particulière doit être accordée au contrôle d'accès physique, aux mesures de sécurité sur le lieu de travail et à la sécurisation du matériel.

L'objectif de cette politique est de prévoir des mesures minimales visant à sécuriser les informations contre l'accès physique non autorisé, la détérioration et la manipulation des informations, ainsi que les installations de traitement de l'information de l'organisation. La politique de sécurisation physique et de sécurisation de l'environnement a été élaborée en tenant compte des normes existantes telles que ISO 27001 et ISO 27002.

Les sociétés de gestion immobilière doivent prendre des mesures pour assurer un niveau minimal de sécurisation. Ces mesures doivent ensuite être communiquées aux organisations qui utilisent les bâtiments. Les organisations qui utilisent des bâtiments doivent intégrer les mesures de gestion des bâtiments dans leur analyse des risques afin de déterminer le niveau de risque. Enfin, les mesures doivent être intégrées dans la politique de l'organisation qui utilise le bâtiment.

Les mesures minimales énoncées dans la présente politique sont liées à une évaluation des risques ou à une analyse d'impact, qui doivent être entreprises par les organisations. Sur la base de cette évaluation des risques, l'organisation peut alors définir un niveau de sécurité souhaité.

Chaque organisation approuve les mesures décrites, pour toutes les informations et tous les systèmes d'information dont elle a la responsabilité. Il importe également de préciser que les mesures minimales proposées concernent la sécurité de l'information et pas les tâches du conseiller en prévention. Toutefois, il est nécessaire qu'il y ait une bonne coopération entre la personne responsable de la sécurité de l'information et le conseiller en prévention. Les procédures et processus de mise en œuvre des mesures doivent être définis et planifiés par l'organisation (par exemple en utilisant ITIL).



Sécurisation des espaces

Généralités

Chaque organisation doit prendre les mesures nécessaires pour prévenir la perte, la détérioration, le vol ou la manipulation des informations dans une organisation. L'organisation doit prendre des mesures physiques conformes aux spécifications et en fonction des bâtiments et des sites.

Les bâtiments et les sites doivent satisfaire aux exigences suivantes en matière d'infrastructures et de dispositions urbanistiques :

1) la résistance aux catastrophes (incendie, foudre, tempêtes, grêle, inondations/fuites d'eau, tremblements de terre, etc.) ;

2) les structures des murs, des sols et des plafonds doivent répondre aux exigences de résistance au feu et être suffisamment finies (poussière, feu, fumée) ;

3) les installations doivent être configurées de manière à empêcher que des informations ou des activités confidentielles ne soient visibles et audibles de l'extérieur ;

4) alimentation électrique externe avec alimentation double face ;

5) la mise en œuvre de mesures contre les dommages causés par une sous-tension ou une surtension ;

Le gestionnaire du bâtiment doit fournir de manière simple toutes les informations relatives à l'infrastructure, aux dispositions urbanistiques et aux solutions aux défaillances techniques.

Alimentation électrique interne

L'approvisionnement interne en électricité est nécessaire dans les zones critiques où les processus d'entreprise les plus critiques doivent être maintenus. Il est également nécessaire d'utiliser un UPS (+ générateur si nécessaire) pour que la tension du réseau ne soit pas défaillante.

Cette installation pour l'alimentation électrique interne doit être testée au moins une fois par an pour s'assurer de son bon fonctionnement. La maintenance de cette installation doit se faire conformément à la réglementation.

Infrastructure de télécommunication

Les points de câblage et de distribution internes de (télé)communication doivent :

1) être inaccessibles aux personnes non autorisées ;

2) être à l'abri des câbles d'alimentation, des paratonnerres, des tubes fluorescents, des bobines, etc.

Des dispositifs de sauvegarde doivent être prévus pour les processus d'entreprise qui nécessitent des connexions de communication de données critiques.

Régulation de l'air ambiant

La régulation de l'air ambiant des différents espaces est essentielle. Le traitement de l'air des espaces critiques où se trouve du matériel sensible doit être séparé des autres espaces. Le risque d'aspiration de substances dangereuses doit également être réduit au minimum. Il faut également tenir compte des fluctuations de température dans les espaces critiques. Enfin, un interrupteur doit être prévu pour que la ventilation de l'air puisse être désactivée manuellement en cas d'alarme.

Protection contre l'incendie

La protection contre l'incendie est soumise à un certain nombre d'exigences en matière de prévention, de détection et de lutte. Ces mesures de sécurisation physique sont inspectées périodiquement.

Dispositions préventives

La propagation du feu et de la fumée doit être limitée en tout temps. Lors de la construction et de l'aménagement des espaces critiques, les matériaux utilisés doivent donc être soigneusement choisis. Des cloisons résistantes au feu sont également essentielles. Les raccordements des murs et des plafonds, le passage des conduits d'air, de l'électricité et d'autres canalisations méritent également une attention particulière (par exemple au moyen de clapets coupe-feu à fermeture étanche à la fumée).

Afin d'éviter les coups de foudre, des installations paratonnerre doivent également être installées pour éviter autant que possible les dommages causés par les coups de foudre.

Enfin, il existe une interdiction légale de fumer dans toutes les organisations - il existe une interdiction de fumer dans tous les espaces (données) critiques.

Détection et signalisation d'incendie

L'équipement de détection automatique (et manuel) doit être présent dans les espaces critiques (également sous les planchers surélevés, au-dessus des plafonds suspendus, etc.) et dans les zones où les exigences de sécurité incendie sont élevées. Le fonctionnement de ces systèmes de détection doit être vérifié régulièrement. En outre, ces systèmes de détection doivent être équipés de leur propre alimentation électrique de secours.

Lutte contre l'incendie

Des instructions de lutte contre l'incendie doivent être fournies afin que chacun sache comment agir en cas d'incendie. Ces instructions accorderont une attention particulière aux éléments suivants :

- la méthode d'alerte et d'évacuation ;
- le sauvetage des supports de données en cours d'utilisation et l'extinction des équipements informatiques ;
- l'utilisation d'extincteurs (automatiques) et des installations de traitement de l'air.

Les espaces critiques doivent être équipés d'un ou de plusieurs systèmes automatiques d'extinction d'incendie. Toutefois, il doit être possible d'éteindre manuellement un incendie. Lors du choix d'un système d'extinction d'incendie, il faut tenir compte du matériel et de la présence éventuelle de collaborateurs et/ou de visiteurs.

Dégâts des eaux

Afin de prévenir les dégâts des eaux dans les espaces critiques, la présence de conduites d'eau dans ces espaces critiques est interdite. De plus, des détecteurs d'humidité automatiques doivent être installés à proximité immédiate du matériel critique. Toutefois, une exception doit être faite pour les systèmes d'extinction d'incendie et les équipements de refroidissement présents dans les centres de données.

Contrôle d'accès physique

L'accès non autorisé à l'information et aux installations de traitement de l'information de l'organisation, ainsi que les dommages occasionnés à celles-ci et l'interférence avec celles-ci, doivent être évités en tout temps.

Étant donné que l'organisation publique est une institution ouverte avec un grand afflux potentiel de personnes et que certains bâtiments ont une fonction publique, une limitation judicieuse de l'accessibilité n'est pas évidente partout.

Les mesures suivantes sont proposées afin d'organiser le flux important d'utilisateurs de manière sûre et conviviale :

1) au moyen de clés (mécaniques ou numériques), selon un plan de fermeture strict ;

2) au moyen de badges d'accès personnels (y compris des badges d'accès temporaires pour les visiteurs).

Les exigences suivantes s'appliquent au contrôle d'accès :

1) Obligation pour les travailleurs de s'identifier. Les badges d'accès sont liées aux personnes. Les badges d'accès vierges ou les badges non attribués doivent être conservés en lieu sûr.

2) L'accès aux zones où des informations confidentielles sont traitées doit être limité aux personnes autorisées. L'accès à ces zones peut être limité par un mécanisme d'authentification composé d'un code PIN pour accéder à l'organisation et d'un badge pour quitter le bâtiment. D'autres possibilités sont la reconnaissance biométrique, le principe des 4 yeux...

3) Les visiteurs doivent être enregistrés au préalable par l'employé d'accueil. Il convient d'indiquer si le visiteur en question peut passer à l'entrée ou doit être pris en charge par l'employé d'accueil.

4) Les visiteurs doivent être enregistrés (date et heure d'arrivée et de départ), par exemple numériquement ou en remplissant un registre des visiteurs.

5) Le personnel de nettoyage et d'entretien non accrédité ne peut travailler dans des zones critiques que sous la supervision permanente d'employés.

6) Surveillance du contrôle d'accès au moyen de caméras de surveillance et/ou de personnel de sécurité.

Zone sécurisée

Après avoir analysé les risques, il peut être plus pratique de créer différentes zones de sécurité dans une organisation. Les zones et les espaces sont ensuite protégés en fonction de leur impact dans l'organisation.

Il serait bon de conclure des accords pratiques mutuels entre les différentes zones. Un « master plan » relatif à la sécurité d'accès ou un document similaire (avec un plan d'approche, des descriptions de processus/procédures, etc.) est certainement approprié ici.

Trois zones globales peuvent être identifiés :

Type	Description
Zone publique	Dans les zones publiques, il n'est pas possible d'effectuer des contrôles physiques suffisants. Il n'est pas possible de garantir le niveau de sécurité requis dans cette zone. Le lieu de travail mobile peut être considéré comme un espace public.
Zone professionnelle	Les zones non publiques, les bâtiments et le lieu de travail font partie de la zone professionnelle. Les espaces couverts par cette zone nécessitent des mesures de sécurité supplémentaires par rapport à la zone publique. Les mesures de sécurité supplémentaires sont prises conformément à la classification DIC (disponibilité, intégrité et confidentialité).
Zones critiques	Il s'agit d'une zone contrôlée avec des mesures de sécurité supplémentaires par rapport à la zone professionnelle. Les mesures de sécurité dépendent notamment de l'impact de la perte, du vol, de la manipulation, etc., des informations sur l'organisation.

Les exigences de sécurité de la zone (zone professionnelle et zone critique)

1) Les zones doivent être séparées les unes des autres sur le plan fonctionnel.

2) Il est interdit d'accorder un accès non autorisé. Des dispositifs de contrôle d'accès doivent être installés pour protéger les zones où se trouvent des informations sensibles ou critiques et des installations TIC.

3) Empêcher ou détecter à temps l'utilisation non autorisée de l'accès aux zones critiques.

4) Le personnel, les visiteurs et les fournisseurs n'ont accès qu'aux zones où leur présence est nécessaire en raison de leurs activités.

5) Il est nécessaire de prévoir des entrées séparées pour les personnes et les marchandises (zones de chargement et de déchargement séparées). Les points d'accès tels que les zones de chargement et de déchargement et les autres points où un accès non autorisé est possible sont contrôlés et, si possible, protégés des zones critiques pour empêcher tout accès non autorisé.

6) Les mesures d'accès pour la sécurisation physique des zones doivent être dotées des mécanismes de contrôle et de surveillance nécessaires :
   - détection de portes ouvertes ;
   - ergot de protection des portes automatiques ;
   - surveillance par caméras ;

- signalisation (incendie, inondation) ;
- protection anti-vol...

7) Le matériel de contrôle d'accès doit être pourvu d'une alimentation électrique de secours pour assurer la sécurité des personnes en cas de panne de courant.

8) La mise en place de processus d'incidents est nécessaire pour assister les personnes présentes (le personnel, les responsables d'immeubles et les visiteurs, le personnel d'accueil et les agents de sécurité...).

Sécurisation du lieu de travail (mobile)

Conjointement aux mesures de sécurisation des sites, les mesures nécessaires doivent également être prises pour le lieu de travail. Le lieu de travail, ou poste de travail, est donc considéré comme un site virtuel.

1) Bureau :

   Au bureau, le lieu de travail utilise indirectement des mesures qui n'ont pas été prises au départ pour le lieu de travail, mais qui offrent une protection supplémentaire. Il s'agit du contrôle d'accès, de la sauvegarde centralisée (protection contre la perte d'informations), de la protection contre l'incendie, de la protection contre les coupures de courant, de la séparation des fonctions, etc.

2) Lieu de travail mobile :

   Sur le lieu de travail mobile, les mesures de sécurité sont généralement moins nombreuses, voire inexistantes. La situation familiale peut être considérée comme un espace public (du point de vue de l'organisation). Une copie de la politique de sécurité relative au matériel situé à l'extérieur de l'organisation doit être remise à l'employé. Il est également nécessaire d'organiser des séances d'information et des campagnes de sensibilisation pour informer les employés.

Architecture du lieu de travail

L'architecture et les mesures de sécurité du lieu de travail doivent tenir compte :

- de l'aspect dynamique du site physique (bureau, en déplacement, pendant le déplacement) ;
- l'aspect mobile du lieu de travail (portables).

Les mesures à prendre s'appliquent aux sites les plus difficiles à sécuriser physiquement :

1) **appareils statiques ;**
   Il s'agit de dispositifs qui ne quittent pas le site physique sécurisé de l'organisation (y compris le réseau sécurisé).
2) **appareils mobiles.**
   Il s'agit de dispositifs qui quittent le site physique sécurisé de l'organisation ou le réseau sécurisé.

Les appareils les plus sensibles sont ceux qui sont pris régulièrement en déplacement ou qui sont régulièrement connectés à un réseau autre que le réseau sécurisé de l'organisation.

Les mesures de sécurité varient selon le type de poste de travail utilisé sur le lieu de travail :

1) Un **appareil kiosque** (non connecté au réseau gouvernemental). Par exemple, un ordinateur connecté à Internet qui est mis à la disposition des visiteurs d'un centre de formation.

2) Un **appareil de bureau** est relié à un réseau gouvernemental et n'a qu'une capacité de traitement limitée. Il est recommandé de ne pas procéder au stockage local des données. L'appareil ne contient que des fonctionnalités génériques et ne sera donc utilisé que pour des applications administratives.

3) Un **appareil spécialisé** est relié à un réseau gouvernemental. Une partie importante du traitement de l'information se fait localement. Des fonctionnalités à la fois génériques et spécialisées auront lieu sur cet appareil (poste de travail pour les développeurs).

Mesures au sein du lieu de travail (mobile)

Mesures contre les pannes de courant.

Si les ordinateurs sont sensibles à une panne de courant et que la continuité du lieu de travail est essentielle, une alimentation de secours peut être utilisée.

Mesures contre le vol.

À l'aide de câbles, de serrures, de protecteurs, etc., les postes de travail fixes peuvent être facilement protégés. Les mesures pour les petits appareils sont davantage nécessaires car ces appareils sont plus faciles à voler (par exemple, un ordinateur portable ou un smartphone). Une attention particulière doit être portée au matériel non géré (par exemple, en se déconnectant en cas d'inactivité sur le réseau ou sur l'appareil). La cryptographie peut être un outil pratique pour empêcher l'accès non autorisé (voir le document Cryptographie).

Traitement des documents

Le traitement des documents sur le lieu de travail (mobile) nécessite également les mesures nécessaires. Les documents non publics doivent être physiquement protégés contre tout accès non autorisé. Les mesures suivantes sont proposées :

- après utilisation, les documents critiques doivent être conservés dans une armoire ignifuge fermant à clé ;
- application des principes du bureau propre et de l'écran verrouillé ;
- les formulaires et badges d'accès vierges doivent être rangés dans une armoire fermant à clé ;
- il est nécessaire d'empêcher la lecture non autorisée de documents, par exemple en utilisant un filtre de sécurité sur les appareils mobiles.

Sécurisation du matériel

En raison des informations stockées dans le matériel, la sécurité de ces informations mérite l'attention nécessaire. Il faut tenter d'éviter que ce matériel ne soit endommagé ou détruit. Il est évident que les mesures de sécurité dépendent des informations qui sont stockées sur ce matériel.

Placement de matériel

Le matériel doit être placé et protégé de manière à réduire les risques de détérioration et de perturbation en provenance de l'extérieur ainsi que les possibilités d'accès non autorisé.

Lors de l'installation de matériel dans un espace, les exigences suivantes doivent être prises en compte :

1) emplacement du matériel ;
   la présence de fenêtres et d'un étage devrait être prise en compte, en vue d'une éventuelle inondation et d'une observation ;

2) accessibilité du matériel ;
   le matériel critique ne peut pas être présent dans les espaces publics ou dans les espaces pouvant être occupés par des employés non autorisés ;

3) placement dans un rack de serveur fermant à clé ;

4) alimentation électrique alternative ;
   la production d'électricité (d'urgence) doit pouvoir garantir l'alimentation en électricité du matériel critique ;

5) protection contre l'interruption de services d'utilité publique ;

6) blindage de câbles d'alimentation et de télécommunications.

Traitement du matériel

Pendant le transport, la mise hors service ou l'entretien du matériel, les mesures de précaution nécessaires doivent être prises pour éviter le vol ou la détérioration. Ceci s'applique non seulement aux serveurs et autre matériel réseau mais aussi aux imprimantes, PC et autres équipements. Les exigences suivantes s'appliquent au matériel :

1) L'entretien, le déplacement ou le transport (en dehors de l'organisation) ne peuvent être effectués que par du personnel autorisé et formé et/ou par des collaborateurs externes.

2) Si le matériel est mis hors service, réutilisé ou transporté hors de l'organisation à des fins de réparation, les données sensibles doivent être effacées afin qu'elles ne puissent plus être reconstituées. La destruction ou l'effacement adéquat de données ou du matériel doit être effectué sur la base d'une évaluation des risques. La mesure appropriée pour l'effacement des données doit faire l'objet d'un contrat (p. ex. leasing, « cloud computing »).

3) Le matériel doit être entretenu conformément aux instructions d'entretien du fournisseur.

4) Le matériel situé à l'extérieur des sites doit être sécurisé, et les utilisateurs doivent prendre des mesures pour protéger le matériel non surveillé.

Lien avec d'autres mesures

Lien avec l'IAM en tant que mesure

La sécurisation de l'accès physique est complémentaire à la gestion de l'accès aux identités (Identity Access Management), comme expliqué dans le document IAM.

Lien avec la journalisation en tant que mesure

La sécurisation physique va généralement de pair avec la journalisation. Il s'agit ici par exemple de :

- la tenue d'un registre ou journal de bord des visiteurs ;
- la tenue d'un journal de bord de l'entretien.

La journalisation manuelle exige la discipline nécessaire pour éviter des erreurs. Le risque d'erreurs est élevé, en partie en raison du nombre d'exécutants concernés.

Les mesures d'atténuation visant à sécuriser les journaux de bord manuels sont notamment les suivantes :

- sécuriser l'accès physique au moyen d'une armoire ignifuge fermant à clé ;
- tenir à jour des copies du journal de bord ;
- numériser et enregistrer en tant que fichier PDF ;
- contrôle et principe des quatre yeux.

Lien avec des exigences régionales et locales en matière de protection contre l'incendie

Les organisations doivent tenir compte des exigences régionales et locales en matière de protection contre l'incendie qu'elles doivent respecter (par exemple, zone Seveso).

Lien avec la séparation des fonctions

Il existe un lien entre la sécurisation de l'information et la séparation des fonctions. La séparation des mesures sur la base des fonctions se fait selon la répartition du travail de l'organisation. Chaque fonction a ses propres mesures spécifiques, qui doivent être exécutées indépendamment les unes des autres.

En général, les séparations de fonctions suivantes s'appliquent :

- entre les tâches d'exécution et les tâches de contrôle ;
- entre la politique et la mise en œuvre ;
- entre la sécurisation physique et la fourniture/sécurisation des TIC.

La sécurisation de l'accès physique vise à protéger les bâtiments et les informations en empêchant l'accès non autorisé. Elle possède sa propre séparation des fonctions :

- propres collaborateurs par rapport aux visiteurs ;
    - les badges visiteurs ne sont délivrés qu'aux personnes qui ne font pas partie de l'organisation ;
- personnel de maintenance externe ;
    - ils ne font pas partie de la propre organisation et doivent être munis d'une carte de visiteur ou d'un autre moyen d'identification ;
- le personnel chargé de l'exécution par rapport au personnel chargé du contrôle ;
    - le personnel d'exécution ne peut en principe pas être autorisé à effectuer des tâches de contrôle (sauf dans le cadre de l'auto-contrôle).

Mise en application

Voir Politique générale de sécurité de l'information.

Gestion du document

Historique

Date	*Auteur*	*Version*	*Description des modifications*
5/04/2019	BOSA	v.0.1	Première ébauche
16/04/2019	BOSA	v.0.2	Mise à jour après révision par le groupe de travail FISP
17/04/2019	BOSA	v.0.3	Mise à jour après révision par le groupe de travail FISP
21/11/2019	FISP workgroup	V.1.0	Distribution publique

Approbations

Date	*Approbateur(s)*	*Version*
21/11/2019	FISP FISP workgroup	V.1.0

Sources

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

- Fysieke controlemaatregelen – Informatieclassificatie Vlaamse overheid
- BIBOSA – 11 – Sécurité physique et sécurité de l'environnement
- IEC27001/2
- Normes minimales, BCSS
- Baseline Security Guidlines, CCB

Lien avec une autre politique

Dépendance de documents internes

Réf.	*Titre*
FISPDOC08	*Aperçu général pour la sécurité de l'information au niveau fédéral*
FISPDOC05	*Guide pour la sécurisation et la gestion des identités et des accès de base (IAM), et des accès privilégiés (PAM)*
FISPDOC03	*Guide pour la cryptographie*

Positionnement de la politique par rapport à la norme ISO 27001

Section	***Objectifs et mesures de référence***	*En relation (X = Oui*
4	*Contexte de l'organisation*	
5	*Leadership*	
6	*Planification*	*x*
7	*Support*	
8	*Fonctionnement*	*x*
9	*Évaluation des performances*	
10	*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)*
A5	*Politique de sécurité de l'information*		
A6	*Organisation de la sécurité de l'information*		
A7	*Sécurité des ressources humaines*		
A8	*Gestion des actifs*		
A9	*Contrôle d'accès*		
A10	*Cryptographie*		
A11	*Sécurité physique et environnementale*	*x*	*11.1 + 11.2*
A12	*Sécurité liée à l'exploitation*		
A13	*Sécurité des communications*		
A14	*Acquisition, développement et maintenance des systèmes d'information*		
A15	*Relations avec les fournisseurs*		

Section	**Objectifs et mesures de référence**	En Relation *(X = Oui)*	Objectifs/Mesures *(Détail)*
A16	*Gestion des incidents liés à la sécurité de l'information*		
A17	*Sécurité de l'information dans la gestion de la continuité de l'activité*		
A18	*Conformité*		