Relations avec les fournisseurs

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences de la norme ISO 27001 : 2022**

**5. Déroulement**

**5.1 Sécurité de l’information dans les relations avec les fournisseurs**

**5.2 Sécurité de l’information dans les accords avec les fournisseurs**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de maintenir un niveau convenu de sécurité de l’information dans les relations avec les fournisseurs.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Relations avec les fournisseurs » s’applique à l’ensemble du personnel ayant des contacts avec les fournisseurs de produits et de services.

**1.3 Glossaire**

SMSI – système de management de la sécurité de l’information

RSI – responsable sécurité de l’information

SI – sécurité de l’information

DCP - données à caractère personnel

TIC – technologie de l’information et de la communication

**2. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application. Il a l’appui du directeur.

**3. Documents**

Gérer la sécurité des fournisseurs

Gérer les services en nuage

Relations avec les fournisseurs

Performance fournisseur

Incidents

Plan de continuité d’activité

Sensibilisation et formation

Transfert de l’information

Continuité d’activité

Classification de l’information

Propriété intellectuelle

Protection de la vie privée

Accord fournisseur

Sécurité de l’information avec les fournisseurs

**4. Exigences de la norme ISO 27001 : 2022**

A.5.19 Relations avec les fournisseurs

Des processus et procédures doivent être définis et appliqués pour gérer les risques de sécurité de l'information liés à l'utilisation de produits et services des fournisseurs.

A.5.20

Les exigences de sécurité de l'information appropriées doivent être mises en place et convenues avec chaque fournisseur, selon le type de relation avec le fournisseur.

**5. Déroulement**

**5.1 Sécurité de l’information dans les relations avec les fournisseurs**

Le processus Gérer la sécurité des fournisseurs est mis en place et respecté afin de maîtriser les risques de sécurité associés à l'utilisation des produits et services fournis par les fournisseurs, y compris les services en nuage, cf. le processus Gérer les services en nuage. Les activités incluent :

* l’identification et la documentation des types de fournisseurs (services TIC, logistique, services publics, services financiers, composants d'infrastructure TIC) qui peuvent affecter la confidentialité, l'intégrité et la disponibilité de l’information de l'organisation
* l’établissement des règles comment évaluer et sélectionner les fournisseurs en fonction de la sensibilité de l’information, des produits et des services (analyse du marché, références des clients, examen de documents, évaluations sur place, certifications)
* l’évaluation et la sélection des produits ou services du fournisseur qui ont des contrôles de sécurité de l'information adéquats et les examiner (exactitude et exhaustivité des contrôles), cf. le document Performance fournisseur
* la définition de l’information de l'organisation, des services TIC et de l'infrastructure physique auxquels les fournisseurs peuvent accéder, surveiller, contrôler ou utiliser
* la définition des types de composants et de services d'infrastructure TIC fournis par les fournisseurs qui peuvent affecter la confidentialité, l'intégrité et la disponibilité de l’information de l'organisation
* l’évaluation et la gestion des risques de sécurité de l'information associés à :
  + l'utilisation par le fournisseur de l’information de l'organisation et des autres actifs associés
  + les risques provenant du personnel potentiellement malveillant du fournisseur
  + au dysfonctionnement ou à la vulnérabilité des produits ou services fournis par le fournisseur
* la surveillance du respect des exigences de sécurité de l'information établies pour chaque type de fournisseur et type d'accès, y compris l'examen par un tiers et la validation du produit
* l’atténuation de la non-conformité d'un fournisseur, que celle-ci ait été détectée par la surveillance ou par un autre moyen
* la gestion des incidents et des imprévus associés aux produits et services du fournisseur, y compris la responsabilité de l'organisation et du fournisseur, cf. la procédure Incidents
* des mesures de résilience et, si nécessaire, de récupération et d'urgence pour garantir la disponibilité de l’information du fournisseur et le traitement de l’information et delà la disponibilité de l’information de l'organisation, cf. le Plan de continuité d’activité
* la sensibilisation et la formation du personnel interagissant avec le personnel du fournisseur concernant les règles d'engagement appropriées, les politiques, processus et procédures spécifiques et le comportement en fonction du type de fournisseur et du niveau d'accès du fournisseur à l’information et système de l’organisation, cf. la procédure Sensibilisation et formation
* la gestion du transfert nécessaire d'information et d'autres actifs associés et tout ce qui doit être changé et s'assurer que la sécurité de l’information est maintenue tout au long de la période de transfert, cf. la procédure Transfert de l’information
* les exigences pour assurer une rupture sécurisée de la relation avec le fournisseur, y compris :
  + la suppression des droits d'accès
  + le traitement de l’information
  + la détermination les droits de propriété intellectuelle développés au cours de la mission
  + la portabilité de l’information en cas de changement de fournisseur ou d'internalisation
  + la gestion des dossiers
  + la restitution des actifs
  + l'élimination sécurisée de l’information et des autres actifs associés
  + les exigences de confidentialité permanentes
* le niveau de sécurité du personnel et de sécurité physique attendu du personnel et des installations du fournisseur

La procédure Continuité d’activité gère la poursuite du traitement de l’information dans le cas où le fournisseur devient incapable de fournir ses produits ou services (fournisseur alternatif).

**5.2 Sécurité de l’information dans les accords avec les fournisseurs**

Les éléments suivants sont pris en compte dans les accords avec les fournisseurs :

* description :
  + de l’information à fournir ou à accéder
  + des méthodes de fourniture ou d'accès
* classification de l’information selon la procédure Classification de l’information
* mise en correspondance entre la classification interne et celle du fournisseur
* le respect des exigences légales, statutaires, réglementaires et contractuelles, y compris la protection des données, le traitement des données à caractère personnel (DCP), les droits de propriété intellectuelle et le droit d'auteur selon les procédures Propriété intellectuelle et Protection de la vie privée
* l'obligation de chaque partie contractante de mettre en œuvre un ensemble convenu de contrôles, y compris le contrôle d'accès, l'examen des performances, la surveillance, le rapport, l'audit
* les obligations du fournisseur de se conformer aux exigences de sécurité de l'information de l'organisation, cf. le fichier Accord fournisseur
* les règles d'utilisation acceptable de l’information et des autres actifs associés
* les conditions d'autorisation et de retrait de l'autorisation d'utilisation de l’information de l'organisation et des autres actifs associés par le personnel du fournisseur (liste explicite du personnel du fournisseur autorisé)
* les exigences de sécurité de l'information concernant l'infrastructure TIC du fournisseur, cf. le fichier Sécurité de l’information avec les fournisseurs
* indemnités et mesures correctives en cas de non-respect des exigences par le contractant
* les exigences et les procédures de gestion des incidents (notification et collaboration lors de la résolution des incidents), cf. la procédure Incidents
* les exigences de formation et de sensibilisation pour les procédures spécifiques et les exigences de sécurité de l'information (réponse aux incidents, procédures d'autorisation)
* les dispositions pertinentes pour la sous-traitance (accord sur l'utilisation de sous-traitants, liste des sous-traitants, notification avant tout changement)
* contacts pertinents (personne de contact pour les questions de sécurité de l'information)
* toute exigence de dépistage, lorsque cela est légalement autorisé, pour le personnel du fournisseur, y compris la responsabilité relative à la conduite des procédures de dépistage et de notification, si le dépistage n'a pas été effectué ou si les résultats suscitent des doutes ou des inquiétudes
* les mécanismes de preuve et d'assurance des attestations de tiers pour les exigences de sécurité de l'information pertinentes liées aux processus du fournisseur et un rapport indépendant sur l'efficacité des contrôles
* droit d'auditer les processus et contrôles du fournisseur liés à l'accord
* obligation du fournisseur de fournir périodiquement un rapport sur l'efficacité des contrôles et accord sur la correction en temps opportun des problèmes pertinents soulevés dans le rapport
* les activités de résolution des défauts et des conflits
* fournir une sauvegarde adaptée aux besoins de l'organisation (fréquence, type et lieu de stockage)
* assurer la disponibilité d'une installation alternative (site de reprise après sinistre) non soumise aux mêmes menaces que l'installation principale et prendre en compte les contrôles de secours (contrôles alternatifs) en cas de défaillance des contrôles primaires
* disposer d'un processus de gestion des modifications qui assure une notification préalable à l'organisation et la possibilité pour l'organisation de ne pas accepter les modifications
* des contrôles de sécurité physique proportionnés à la classification de l’information
* contrôles du transfert de l’information pour la protéger pendant le transfert physique ou la transmission électronique
* les clauses de résiliation à la conclusion de l'accord, y compris la gestion des dossiers, la restitution des actifs, l'élimination sécurisée de l’information et des autres actifs associés, et toute obligation de confidentialité en cours
* mise à disposition d'une méthode de destruction sécurisée de l’information de l'organisation stockée par le fournisseur dès qu'elle n’est plus nécessaire
* assurer, à la fin du contrat, le transfert du support à un autre fournisseur ou à l'organisation elle-même