Utilisation des services en nuage

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique utilisation des services en nuage**

Historique

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

**1. Objet**

La politique utilisation des services en nuage a pour objet de décrire les méthodes utilisées afin de maîtriser les services en nuage utilisés par notre organisation.

**2. Finalité**

La politique utilisation des services en nuage a pour finalité de spécifier et de gérer la sécurité de l’information pour l'utilisation des services en nuage.

**3. Domaine d’application**

La politique utilisation des services en nuage s’applique à tous les départements utilisant les services en nuage.

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de la politique utilisation des services en nuage. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département.

**5. Documents**

Relations avec les fournisseurs

Chaîne TIC

Accord fournisseur

Résultats d’appréciation des risques

Résultats du traitement des risques

Programmes malveillants

Contrôle d’accès

Collecte de preuves

Sauvegarde

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

A.5.23 Sécurité de l’information dans l’utilisation de services en nuage

Les processus d'acquisition, d'utilisation, de gestion et de cessation des services en nuage doivent être établis conformément aux exigences de sécurité de l'information de l'organisation.

**7. Politique utilisation des services en nuage**

La politique utilisation des services en nuage est communiquée à toutes les parties intéressées concernées.

L'organisation établit la manière dont elle entend gérer les risques de sécurité de l'information associés à l'utilisation des services en nuage. Cela fait partie de la gestion des fournisseurs et de la chaîne TIC, cf. les procédures Relations avec les fournisseurs et Chaîne TIC.

L'utilisation de services en nuage implique des responsabilités spécifiques pour la sécurité de l’information du fournisseur de services en nuage et de l'organisation.

Les éléments suivant sont définis :

* toutes les exigences pertinentes en matière de sécurité de l’information associées à l'utilisation des services en nuage
* les critères de sélection du service en nuage et l'étendue de l'utilisation du service en nuage
* les rôles et responsabilités liés à l'utilisation et à la gestion des services en nuage
* quelles mesures de sécurité de l’information sont gérées par le fournisseur de services en nuage et lesquelles sont gérées par l'organisation (en tant que client)
* comment obtenir et utiliser les fonctionnalités de sécurité de l’information fournies par le fournisseur de services en nuage
* comment obtenir une assurance sur les mesures de sécurité de l’information mis en œuvre par les fournisseurs de services en nuage
* comment gérer les contrôles, les interfaces et les changements de services lorsqu'une organisation utilise plusieurs services en nuage, en particulier de différents fournisseurs
* les procédures de gestion des incidents de sécurité de l'information qui peuvent se produire par l'utilisation des services en nuage
* l’approche de surveillance, de revue et d'évaluation de l'utilisation continue des services en nuage pour gérer les risques de sécurité de l'information
* comment modifier ou arrêter l'utilisation des services en nuage, y compris les stratégies de sortie des services en nuage

Les accords de service en nuage sont souvent prédéfinis et non ouverts à la négociation, cf. le fichier Accord fournisseur. Pour tous les services en nuage, l'organisation examine les accords de service en nuage avec le(s) fournisseur(s) de services.

Un accord de service en nuage traite les exigences de confidentialité, d'intégrité, de disponibilité et de traitement de l’information, avec des objectifs de niveau de service en nuage et des objectifs qualitatifs de service en nuage appropriés.

Les évaluations des risques identifiés liés à l'utilisation du service en nuage sont entreprises. Tout risque résiduel lié à l'utilisation du service en nuage est clairement identifié et accepté par la direction, cf. les fichiers Résultats d’appréciation des risques et Résultats du traitement des risques.

L’accord entre le fournisseur de services en nuage et l'organisation (en tant que client) afin de protéger les données de l’organisation et la disponibilité des services inclut les éléments suivants :

* fournir des solutions basées sur les normes acceptées par l'industrie pour l'architecture et l'infrastructure
* gérer les contrôles d'accès du service en nuage afin de répondre aux exigences de l'organisation selon la procédure Contrôle d’accès
* mettre en place des solutions de surveillance et de protection contre les logiciels malveillants selon la procédure Programmes malveillants
* traiter et stocker les informations sensibles de l'organisation dans des emplacements approuvés (pays ou région en particulier) ou soumis à une juridiction particulière
* fournir une assistance dédiée en cas d'incident de sécurité de l'information dans l'environnement de service en nuage
* s'assurer que les exigences de l'organisation en matière de sécurité de l’information sont respectées en cas de sous-traitance ultérieure des services en nuage à un fournisseur externe (ou interdire la sous-traitance des services en nuage)
* soutenir la collecte de preuves numériques, en tenant compte des lois et réglementations relatives aux preuves numériques dans différentes juridictions selon la procédure Collecte de preuves
* fournir une assistance et une disponibilité des services appropriées pendant la période pendant laquelle l'organisation souhaite quitter le service en nuage
* fournir la sauvegarde requise des données et des informations de configuration selon la procédure Sauvegarde
* fournir et renvoyer des informations telles que les fichiers de configuration, le code source et les données appartenant à l'organisation (en tant que client), sur demande lors de la fourniture du service ou à la fin du service

L'organisation, en tant que client du service en nuage détermine si l'accord doit exiger du fournisseur de services en nuage qu’il fournisse une notification préalable avant que tout changement important ne soit apporté à la manière dont le service est fourni comme :

* des modifications de l'infrastructure technique (relocalisation, reconfiguration ou modification du matériel ou des logiciels) qui affectent ou modifient l'offre de services en nuage
* traiter ou stocker des informations dans une nouvelle juridiction géographique ou juridique
* l'utilisation de fournisseurs de services en nuage homologues ou d'autres sous-traitants

L'organisation utilisant les services en nuage maintien un contact étroit avec ses fournisseurs. Ces contacts permettent l'échange mutuel d'informations sur la sécurité de l’information pour l'utilisation des services en nuage, y compris un mécanisme permettant à la fois au fournisseur de services en nuage et à l'organisation, en tant que client, de surveiller chaque caractéristique du service et de signaler les manquements aux engagements contenus dans le les accords.