Installation de logiciels

**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**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité d’assurer l’intégrité des systèmes opérationnels et d’empêcher l'exploitation des vulnérabilités techniques.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Installation de logiciels » s’applique aux personnes responsables de l'installation de logiciels opérationnels.

**1.3 Glossaire**

SI – sécurité de l’information

RSI – responsable sécurité de l’information

**2. Responsabilité**

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

**3. Documents**

Authentification

Plan de test

Inventaire des actifs

Gestion des vulnérabilités

Activités de surveillance

Relations avec les fournisseurs

Demande de changement

Mot de passe

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

A.8.19 Installation de logiciels

Des procédures et des mesures doivent être mises en place pour gérer de manière sécurisée l'installation de logiciels opérationnels.

**5 Déroulement**

Des règles strictes sur les types de logiciels que les utilisateurs peuvent installer et utiliser sont définies et respectées.

Pour gérer en toute sécurité les modifications et l'installation de logiciels sur les systèmes opérationnels les éléments suivants sont pris en compte :

* effectuer les mises à jour du logiciel opérationnel uniquement par des administrateurs formés et avec une authentification appropriée, cf. la procédure Authentification
* s'assurer que seul le code exécutable approuvé et aucun code de développement ou compilateur ne sont installés sur les systèmes opérationnels
* installer et mettre à jour le logiciel uniquement après des tests approfondis et réussis selon le Plan de test
* mettre à jour toutes les bibliothèques de sources de programmes correspondantes
* utiliser un système de contrôle de configuration pour garder le contrôle de tous les logiciels opérationnels ainsi que de la documentation du système, cf. le fichier Inventaire des actifs
* définir une stratégie de restauration avant la mise en œuvre des modifications
* maintenir un journal d'audit de toutes les mises à jour du logiciel opérationnel
* archiver les anciennes versions du logiciel, ainsi que toutes les informations et paramètres requis, les procédures, les détails de configuration et le logiciel de support en tant que mesure d'urgence, et aussi longtemps que le logiciel est nécessaire pour lire ou traiter les données archivées

Toute décision de mise à niveau vers une nouvelle version prend en compte les exigences commerciales pour le changement et la sécurité de la version. Les correctifs logiciels sont appliqués lorsqu'ils peuvent aider à supprimer ou à réduire les vulnérabilités de la sécurité de l’information, cf. la procédure Gestion des vulnérabilités.

Les logiciels et progiciels fournis en externe sont surveillés et contrôlés pour éviter les modifications non autorisées, car ils peuvent introduire des vulnérabilités en matière de sécurité de l’information, cf. la procédure Activités de surveillance.

Les logiciels fournis par le fournisseur et utilisés dans les systèmes opérationnels sont maintenus à un niveau pris en charge par le fournisseur. L'organisation tient compte des risques liés à l'utilisation de logiciels non pris en charge.

Les logiciels open source utilisés dans les systèmes opérationnels sont maintenus jusqu'à la dernière version appropriée du logiciel. L'organisation tient compte des risques liés à l'utilisation de logiciels open source non maintenus lorsqu'ils sont utilisés dans des systèmes opérationnels.

Lorsqu’un fournisseur est impliqué dans l'installation ou la mise à jour du logiciel, l'accès physique ou logique ne doit être accordé qu'en cas de nécessité et avec l'autorisation appropriée. Les activités du fournisseur sont gérées selon la procédure Relations avec les fournisseurs.

Le principe du moindre privilège est appliqué à l'installation de logiciels sur des systèmes opérationnels.

L'organisation identifie les types d'installations logicielles autorisées (mises à jour et correctifs de sécurité des logiciels existants) et les types d'installations interdites (logiciels destinés uniquement à un usage personnel et logiciels potentiellement malveillants ou suspects).

La gestion des mises à jour logicielles est appliqué afin de garantir que les correctifs approuvés et les mises à jour d'application les plus récents soient installés pour tous les logiciels autorisés.

Si des modifications sont nécessaires, le logiciel d'origine est conservé et les modifications appliquées à une copie désignée. Toutes les modifications sont entièrement testées et documentées, afin qu'elles puissent être réappliquées, si nécessaire, aux futures mises à niveau logicielles. Si nécessaire, les modifications sont testées et validées par un organisme d'évaluation indépendant.

Toute installation de nouveaux systèmes, logiciels et applications demande une validation et autorisation personnalisées (par exemple RSI et directeur).

Les nouvelles fonctionnalités ou changements de fonctionnalités liées à un nouveau système ou à une nouvelle version sont systématiquement décrites dans une Demande de changement.

Une analyse des spécifications en matière de sécurité de l'information est réalisée par le RSI.

Le RSI vérifie qu’aucune restriction n’empêche l’installation du nouveau logiciel et s’assure de l’absence d'erreurs dues au fonctionnement du logiciel.

Avant l’acceptation du logiciel celui-ci est soumis à un test de sécurité pour garantir qu’aucune conséquence négative n’apparait dans les autres systèmes et applications. Le RSI scanne tous les logiciels pour détecter les virus avant leur installation. Cela comprend aussi les logiciels sous emballage plastique achetés directement auprès de nos partenaires commerciaux.

La revue des nouvelles fonctionnalités (ou des changements de fonctionnalités) liées à un changement majeur de logiciel ou système comprend une analyse des nouveaux risques. Cette revue est parfois menée en partenariat avec une équipe externe.

Le département SI conserve dans l’Inventaire des actifs la liste des versions en vigueur des logiciels et applications sur chaque poste utilisateur.

Le changement de mots de passe par défaut des nouveaux logiciels est une règle qu’il faut appliquer systématiquement, cf. le fichier Mot de passe.