Accès au code source

**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’empêcher l'introduction de fonctionnalités non autorisées, d’éviter les modifications involontaires ou malveillantes et de maintenir la confidentialité de la propriété intellectuelle de valeur.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Accès au code source » s’applique aux personnes ayant un accès privilégié au code source, aux outils de développement et aux bibliothèques de logiciels.

**1.3 Glossaire**

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. Il est garant de son application. Il a l’appui du directeur.

**3. Documents**

Changements

Enregistrements

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

A.8.4 Accès au code source

L'accès en écriture et en lecture au code source, aux outils de développement et aux bibliothèques de logiciels doit être géré de manière appropriée.

**5. Déroulement**

L'accès au code source et aux éléments associés (spécifications, plans de vérification et de validation) et aux outils de développement (compilateurs, outils d'intégration, environnements de test) est strictement contrôlé. Cela peut être réalisé en contrôlant le stockage central du code.

L'accès en lecture et en écriture au code source diffère en fonction du rôle du personnel. L'accès en lecture au code source est largement autorisé en interne. L'accès en écriture au code source n'est disponible qu'au personnel privilégié.

Lorsque les composants de code sont utilisés par plusieurs développeurs en interne, un accès en lecture à un référentiel de code centralisé est mis en œuvre. Cependant, l'accès en écriture est toujours restreint.

Les éléments suivants sont pris en compte pour maîtriser l'accès aux bibliothèques de sources de programmes :

* gérer l'accès au code source du programme et aux bibliothèques selon les procédures établies
* accorder un accès en lecture et en écriture au code source en fonction des besoins de l'entreprise
* traiter les risques d'altération ou d'utilisation abusive selon les procédures établies
* mettre à jour le code source et les éléments associés et octroyer l'accès au code source selon la procédure Changements seulement après autorisation appropriée
* ne pas accorder aux développeurs un accès direct au répertoire du code source, mais via des outils de développement qui contrôlent les activités et les autorisations reçues
* conserver les listes de programmes dans un environnement sécurisé, où l'accès en lecture et en écriture est géré de manière appropriée
* maintenir un journal d'audit de tous les accès et de toutes les modifications apportées au code source selon la procédure Enregistrements

Quand le code source est destiné à être publié, des contrôles supplémentaires pour garantir son intégrité (signature numérique) sont envisagés.

Quand l'accès au code source n'est pas correctement contrôlé, certaines données de l'environnement du développement peuvent être récupérées par des personnes non autorisées.