Changements

**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 Demande de changement**

**5.2 Analyse préalable**

**5.3 Tests**

**5.4 Accord du changement**

**5.5 Changement de documents**

**5.6 Application du changement**

**5.7 Gestion de la configuration**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de :

* préserver la sécurité de l’information lors de l'exécution des changements
* de garantir que le matériel, les logiciels, les services et les réseaux fonctionnent correctement avec les paramètres de sécurité requis et que la configuration n'est pas altérée par des changements non autorisées ou incorrectes

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Changements » s’applique à tous les systèmes, réseaux, ordinateurs, logiciels et applications utilisés dans notre organisation.

**1.3 Glossaire**

RSI – responsable sécurité de l’information

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**

Codage

Sécurité de l’information

Plan de continuité d’activité

Continuité d’activité

Demande de changement

Plan de test

Procédures

Enregistrements

Séparation des environnements

Gérer la configuration

Registre des licences

Registre de la configuration

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

A.8.32 Changements

Les changements des moyens de traitement de l'information et des systèmes d'information doivent être appliqués selon des procédures de gestion des changements.

A.8.9 Gestion de la configuration

Les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux, doivent être définies, documentées, appliquées, surveillées et revues.

**5. Déroulement**

**5.1 Demande de changement**

Une demande de changement est proposée quand :

* un processus (produit) doit être changé suite à une demande client
* une opportunité d’amélioration a été identifiée suite à un audit
* des actions correctives doivent être appliquées suite à l’identification de non-conformités
* un produit doit être actualisé suite à de nouvelles conditions d’utilisation

Plus de détails dans la procédure Codage.

Tout changement concerne de près ou de loin la politique de Sécurité de l’information. La demande de changement est toujours d’un utilisateur autorisé et précise :

* l’objet du changement
* le motif du changement (sécurité, qualité, fiabilité, fonctionnalité, standardisation, prix, délai...)
* le délai souhaité d'application

Tout changement important est traité comme l’application d'un nouveau système et sera considéré comme un nouveau projet. La confidentialité, l’intégrité et la disponibilité de l’information est assurée tout au long du cycle de vie du projet. Le Plan de continuité d’activité sera actualisé. Plus de détails dans la procédure Continuité d’activité.

**5.2 Analyse préalable**

La demande de changement est analysée par le RSI, notamment en termes de faisabilité technique, de risque, de délai d’application et de coût. En cas de problème, le RSI négocie une modification de la demande de changement. La Demande de changement est vérifiée par les membres de l’équipe sécurité de l’information. Une analyse des risques et une évaluation des impacts sont réalisées. Les différents départements concernés par le changement sont informés. Les départements concernés valident le changement en précisant les éventuelles difficultés. Il s’agit :

* d’évaluer :
  + les bénéfices
  + l’urgence
  + les délais d’application
  + les coûts
* de déterminer l’impact de l’application du changement sur la sécurité de l’information

**5.3 Tests**

Le RSI soumet le changement à des tests de simulation pour écarter toute conséquence indésirable sur les autres systèmes ou applications et l’enregistre dans le fichier Plan de test.

**5.4 Accord du changement**

Quand la demande vient du client après avoir analysé les différentes remarques des départements concernés, le RSI donne son accord au client en lui précisant les délais et conséquences de l’application du changement. En cas de désaccord, le RSI peut impliquer le commercial pour négociation commerciale.

Pour les demandes internes après avoir analysé les différentes remarques des départements concernés, le RSI donne son accord pour l’application du changement.

**5.5 Changement de documents**

Quand le changement nécessite une mise à jour d’un ou plusieurs documents la révision des documents est réalisée selon les procédures Procédures et Enregistrements.

Tous les utilisateurs concernés sont informés du changement.

**5.6 Application du changement**

Après avoir reçu toutes les informations, les différents départements précisent la date d’application du changement. Chaque département lance alors les démarches nécessaires à l’application du changement (révision des documents, du logiciel, de l’application).

Les changements appliqués sont enregistrés dans le fichier Demande de changement.

Peu de temps après l’application une surveillance du changement est réalisée et son efficacité est évaluée.

Le changement de logiciel peut avoir un impact sur l'environnement de production et vice versa.

Les bonnes pratiques incluent le test des composants TIC dans un environnement séparé des environnements de production et de développement selon la procédure Séparation des environnements.

**5.7 Gestion de la configuration**

Le processus Gérer la configuration définit les actions et outils pour appliquer la gestion de la configuration du matériel, des logiciels, des services (services en nuage) et des réseaux, pour les systèmes nouvellement installés ainsi que pour les systèmes opérationnels tout au long de leur durée de vie.

Des modèles normalisés pour la configuration sécurisée sont définis et les éléments suivants sont pris en compte :

* utiliser des conseils accessibles au public (modèles prédéfinis de fournisseurs et d'organisations de sécurité indépendantes)
* considérer le niveau de protection nécessaire afin de déterminer un niveau de sécurité suffisant
* soutenir la politique de sécurité de l'information de l'organisation, les politiques spécifiques à un sujet, les normes et les autres exigences de sécurité
* examiner la faisabilité et l'applicabilité des configurations de sécurité dans le contexte de l'organisation

Les modèles sont revus périodiquement et mis à jour lorsque de nouvelles menaces ou vulnérabilités doivent être traitées, ou lorsque de nouvelles versions logicielles ou matérielles sont introduites.

Les éléments suivants sont pris en compte afin d’établir des modèles pour la configuration sécurisée du matériel, des logiciels, des services et des réseaux :

* minimiser le nombre d'identités avec des droits d'accès de niveau privilégié ou administrateur
* désactiver les identités inutiles, inutilisées ou non sécurisées
* désactiver ou restreindre les fonctions et services inutiles
* restreindre l'accès aux programmes utilitaires puissants et aux réglages des paramètres
* synchroniser les horloges
* modifier les informations d'authentification par défaut du fournisseur telles que les mots de passe par défaut immédiatement après l'installation
* examiner d'autres paramètres importants liés à la sécurité par défaut
* avoir recours à des installations de temporisation (déconnexion automatiquement des dispositifs informatiques après une période d'inactivité prédéterminée)
* vérifier que les exigences de licence sont respectées, cf. Registre des licences

Les configurations établies du matériel, des logiciels, des services et des réseaux sont enregistrées dans le Registre de la configuration.

Les changements apportés aux configurations sont gérés comme les autres changements.

Les enregistrements de configuration peuvent contenir, selon le cas :

* informations à jour sur le propriétaire ou le point de contact pour l'actif
* date du dernier changement de configuration
* version du modèle de configuration
* relation avec les configurations d'autres actifs

Les configurations sont surveillées à l'aide d'outils de gestion du système (utilitaires de maintenance, assistance à distance, outils de gestion d'entreprise, logiciels de sauvegarde et de restauration).

Les configurations sont examinées régulièrement afin de vérifier :

* les paramètres de configuration
* évaluer la force des mots de passe
* évaluer les activités effectuées

Les configurations réelles peuvent être comparées aux modèles cibles définis. Tout écart est traité, soit par l'application automatique de la configuration cible définie, soit par une analyse manuelle de l'écart suivie d'actions correctives.

Les modèles de configuration et les cibles peuvent être des informations confidentielles et sont dans ce cas protégés contre tout accès non autorisé.