Procédure de contrôle des informations documentée ISMS ISO 27001:2022

Indice

1 Présentation

Les « informations documentées » sont définies par l'ISO comme « les informations devant être contrôlées et conservées par une organisation et le support sur lequel elles sont contenues ». Ce terme recouvre ce que l'on appelait autrefois « documents et enregistrements » et, dans un souci de clarté, cette procédure fait toujours la distinction entre ces deux types d'informations documentées.

L'utilisation d'informations documentées est une partie essentielle du système de gestion de la sécurité de l'information (SMSI) afin d'établir l'intention de la direction, de fournir des indications claires sur la manière dont les choses doivent être faites et de fournir des preuves des activités qui ont été réalisées .

La norme ISO/IEC 27001 exige que toutes les informations documentées composant le SMSI soient vérifiées pour s'assurer qu'elles sont disponibles et adaptées à l'utilisation, où et quand cela est nécessaire, et qu'elles sont protégées de manière adéquate. Un tel contrôle est essentiel pour s'assurer que les processus et procédures corrects sont toujours utilisés au sein de l'organisation et qu'ils restent adaptés à l'objectif pour lequel ils ont été créés.

Les principes généraux énoncés dans la norme et retenus dans cette procédure sont que toute information documentée doit être :

- Facilement identifiable et disponible
- Daté et autorisé par une personne désignée
- Lisible
- Maintenu sous contrôle de version et disponible pour toutes les personnes et tous les lieux où les activités pertinentes sont effectuées
- Retiré rapidement lorsqu'il est obsolète et conservé si nécessaire à des fins légales ou de préservation des connaissances

Cette procédure détermine comment ce niveau de contrôle sera atteint au sein de [Nom de l'entreprise] .

2 Procédure de contrôle des documents

Cette procédure s'applique aux « documents » (par opposition aux « enregistrements » couverts ci-dessous) qui sont généralement créés via un traitement de texte (ou une application bureautique similaire) et décrivent l'intention de la direction, comme les politiques, les plans et les procédures .

2.1 Aperçu

Le processus général de contrôle des documents est illustré dans le schéma ci-dessous.

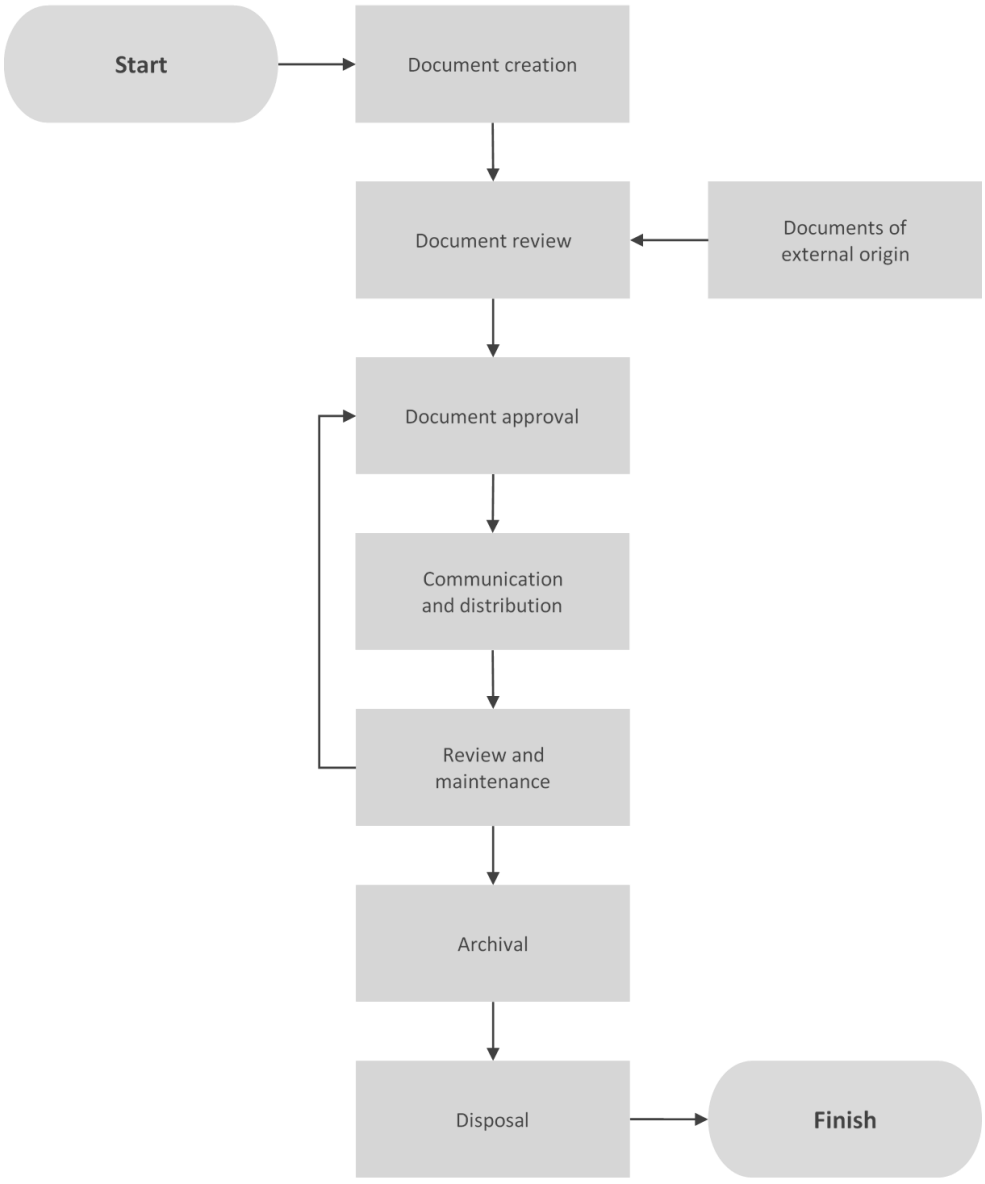

Figure 1 : Procédure de contrôle des documents

Chacune de ces étapes est décrite plus en détail dans les sections restantes de cette procédure.

2.2 Création de documents

équipe de direction de [Nom de l'entreprise] et pourra être entreprise par toute personne compétente appropriée au sujet et au niveau du document. Cependant, plusieurs règles doivent être suivies lors de la création d'un document à utiliser dans le SMSI.

2.2 .1 Convention de nommage

La convention de dénomination des documents dans le SMSI prévoit l'utilisation du format suivant :

SGSI-PROC-xx- yy(- zz) - Titre du document Rev Status dd

Où

- **SMSI** : Système de management de la sécurité de l'information
- **PROC** : Document
- **xx** : référence du domaine thématique (voir tableau 1)
- **yy** : numéro de document unique (ou, pour les contrôles, une référence de contrôle)
- **zz** : Pour les chèques uniquement, un numéro de document unique
- **Titre du document** : description significative du document
- **Rév** : numéro de révision
- **Statut** : Statut du document (Brouillon ou Final)
- **Dd** : numéro de brouillon, le cas échéant

Un numéro unique sera attribué à chaque document et un index des références de documents sera conservé dans le système de qualité ISMS - voir le registre de documentation du système de gestion de la sécurité de l'information pour plus de détails.

Les références des domaines sont conçues pour correspondre aux sections de la norme ISO/IEC 27001 comme suit (des domaines supplémentaires peuvent être créés si nécessaire) :

Référence au domaine	Domaine ISO/CEI 27001
00	Présentation du projet et ressources

Référence au domaine	Domaine ISO/CEI 27001
01	Portée
02	références réglementaires
03	Termes et définitions
04	4. Contexte de l'organisation
05	5. Orientation
06	6. Planification
07	7. Assistance
08	8. Fonctionnement
09	9. Évaluation des performances
dix	10. Amélioration
A05	A5. Contrôles organisationnels
A06	A6. Contrôles des personnes
A07	A7. Contrôles physiques
A08	A8. Contrôles technologiques

Tableau 1 : Références au domaine thématique du document

2.2.2 Contrôle des versions

Les numéros de version des documents seront composés d'un numéro majeur uniquement. Par exemple, V2 est la version 02.

Lorsqu'un document est créé pour la première fois, il aura un numéro de version de 01 et sera à l'état Brouillon. Chaque fois qu'un brouillon est distribué, toute autre modification entraînera une augmentation du numéro de brouillon de 01, par exemple de 01 à 02.

Par exemple, lorsqu'un document est créé pour la première fois, il s'agira de la version 1 brouillon 01. Un deuxième brouillon sera V1 brouillon 02, etc. Une fois le document approuvé, il deviendra V1 Finale.

Le numéro de version sera incrémenté lors de la création d'une version préliminaire ultérieure.

Par exemple, une révision de document approuvée qui est en V1 Final sera V2 Draft 01 puis V2 Draft 02 etc. jusqu'à ce qu'il soit approuvé lorsqu'il deviendra V2 Final.

Les documents doivent inclure un historique de révision comme suit :

Version	Date	Auteur de la revue	Sommaire des changements

Tableau 2 : Historique des révisions

Une fois que le document atteint sa version finale, seules les versions approuvées doivent être enregistrées dans ce tableau.

2.2.3 Statut du document

L'état reflète l'étape à laquelle se trouve le document, comme suit :

- Ébauche : en cours d'élaboration et de discussion, c'est-à-dire qu'elle n'a pas été approuvée
- Final : après approbation et publication dans l'environnement de travail réel

2.2.4 Documents d'origine externe

Les documents qui proviennent de l'extérieur de l'organisation, mais qui font partie du SMSI, recevront une page de référence et d'en-tête jointe au début du document, détaillant les informations normalement incluses dans les documents internes, telles que :

- Référence au document
- Version
- Date
- Statut
- Diffusion

Ces documents seront donc soumis aux mêmes contrôles que ceux qui arrivent en interne.

2.3 Examen du document

Les projets de documents seront examinés par un niveau et un nombre d'employés appropriés au contenu et au sujet du document.

Les lignes directrices sont les suivantes :

Type de document	Réviseurs
Stratégie	[Nom/titre de l'examinateur]
Politique	[Nom/titre de l'examinateur]
Procédure	[Nom/titre de l'examinateur]
Sol	[Nom/titre de l'examinateur]

Tableau 3 : Lignes directrices pour l'examen des documents

Une fois approuvée, la date de la prochaine révision prévue doit être enregistrée dans le *registre de documentation du système de gestion de la sécurité de l'information* .

2.4 Approbation du document

Tous les documents doivent passer par un comité d'approbation pour s'assurer qu'ils sont corrects, adaptés à l'usage et produits conformément aux directives locales de contrôle des documents. Les conseils seront différents selon le type de document et pourront être divisés en plusieurs groupes avant d'être approuvés.

De manière standard, les commissions d'agrément sont :

Type de document	Approbateurs
Stratégie	[Nom/titre de l'approbateur]
Politique	[Nom/titre de l'approbateur]
Procédure	[Nom/titre de l'approbateur]
Sol	[Nom/titre de l'approbateur]

Tableau 4 : Frais d'approbation des documents

Chaque document qui nécessite une approbation doit avoir un tableau comme indiqué ci-dessous :

Prénom	Position	Signature	Date

Tableau 5 : Approbation du document

Une fois approuvé, une copie du document doit être imprimée et signée par l'approbateur. [Remarque : Vous pouvez choisir de le faire par voie électronique plutôt que d'imprimer une copie] . Cette copie sera ensuite conservée dans une archive centrale

Lors de l'approbation d'une nouvelle version d'un document, tous les détenteurs de versions antérieures seront invités à obtenir une nouvelle version et à détruire l'ancienne.

2.5 Communications et diffusion

Une liste de diffusion sera incluse comme suit :

Prénom	Titre

Tableau 6 : Liste de diffusion

Cette liste doit être précise car elle servira de base pour informer les utilisateurs du document qu'une nouvelle version est maintenant disponible.

2.6 Examen et conservation des documents

Tous les documents finaux doivent être archivés électroniquement et sur papier à la fois localement et hors site pour s'assurer qu'ils sont accessibles dans toutes les situations.

Les documents ISMS sont stockés électroniquement sur le disque partagé dans son sous-dossier (par exemple, les responsabilités de gestion, la revue de direction, etc.). Le lecteur est un lecteur partagé auquel tous les membres appropriés de Nom de l'organisation ont accès , conformément aux politiques de contrôle d'accès publiées.

Les documents finaux sont archivés en format papier dans une structure d'archives qui imite la version électronique. [Indiquer l'emplacement des archives papier].

Une copie intégrale de la documentation finale sera reproduite et conservée dans la médiathèque définitive.

2.7 Conservation des documents

Les documents approuvés qui dépassent leur durée de vie utile sont stockés dans un dossier remplacé sur le disque partagé pour former une piste d'audit du développement et de

l'utilisation des documents. Ils doivent être marqués comme remplacés pour éviter qu'ils ne soient utilisés par erreur comme une version plus récente.

2.8 Élimination des documents

Les copies papier des documents approuvés qui ont été remplacés doivent être éliminées dans des conteneurs sécurisés ou déchiquetées, conformément aux *procédures de gestion des actifs convenues* .

3 Cycle de vie des enregistrements

Cette section décrit la vérification du type d'informations documentées qui montrent généralement ce qui a été fait, comme un « journal » d'activité, tel qu'un formulaire rempli, un journal de sécurité ou un rapport de réunion.

3.1 Identification

Il existe une variété de types d'enregistrements qui peuvent faire partie du SMSI et ceux-ci seront associés aux processus spécifiques impliqués, tels que :

- Incidents de sécurité
- Demandes de modification
- Éléments de configuration
- Journaux des événements de sécurité

De plus, il y aura des éléments plus généraux tels que les procès-verbaux de réunion qui pourraient être appliqués à tous les processus. En termes d'identification, dans de nombreux cas, cela sera dicté par l'outil créant l'enregistrement, par exemple l'outil utilisera un système de numérotation unique tel que INC000001 pour les incidents de sécurité ou CHG000001 pour les modifications.

Pour les enregistrements créés manuellement, les règles suivantes s'appliquent :

1. Les procès-verbaux des réunions seront nommés en fonction du sujet de la réunion et de la date
2. Les rapports seront nommés en fonction du sujet du rapport et de la période de rapport
3. Les journaux seront nommés avec le titre du journal et la date/heure de la période couverte

Pour tous les autres types d'enregistrements non couverts, le créateur doit faire preuve de bon sens pour s'assurer que le nom choisi donne une bonne indication du contenu du fichier et doit être conservé dans un endroit correspondant à son objectif.

3.2 Stockage

De nombreux enregistrements du SMSI seront stockés dans des bases de données d'application spécialement conçues, telles que la base de données des incidents de sécurité.

Pour les enregistrements hors base de données, une structure de classement logique sera créée en fonction du domaine ISMS concerné.

[Décrivez l'installation de stockage sur votre serveur où vous stockerez vos enregistrements ISMS]

Dans la mesure du possible, tous les dossiers seront conservés électroniquement ; les documents papier doivent être numérisés si une copie électronique originale n'est pas disponible.

3.3 Protection

Les enregistrements conservés dans les bases de données de l'application feront l'objet de sauvegardes régulières conformément à la politique de sauvegarde convenue. Les zones de stockage de fichiers seront également sauvegardées régulièrement, toutes les sauvegardes les plus récentes étant conservées dans un emplacement hors site.

L'accès aux journaux sera limité aux personnes autorisées conformément à la *politique de contrôle d'accès* de [Nom de l'entreprise] .

3.4 Récupération

Les enregistrements seront généralement récupérés via l'application qui les a créés, comme le système de centre de services pour les incidents de sécurité et un observateur d'événements pour les journaux.

Des outils de reporting seront également utilisés pour traiter et consolider les données en informations significatives.

3.5 Conservation

La durée de conservation des enregistrements dans le SMSI dépendra de leur utilité pour [Nom de l'entreprise] et de toute contrainte légale, réglementaire ou contractuelle. Les enregistrements du centre de services liés à la sécurité sont utiles pour analyser les tendances historiques et seront

donc conservés pendant une période d' au moins sept ans . Des précautions seront prises au cas où des documents pourraient avoir une certaine pertinence commerciale en cas de litige, tels que des contrats et des procès-verbaux de réunion avec des fournisseurs, et ceux-ci devraient être conservés pendant la même durée .

Les enregistrements particulièrement détaillés et uniquement pertinents pour une courte période, tels que les journaux d'événements du serveur, ne doivent être conservés qu'en cas de besoin immédiat.

Des périodes de conservation spécifiques sont définies dans la Politique de conservation et de protection des documents.

3.6 Élimination

De nombreux systèmes utilisent le concept d'archivage et, dans la plupart des cas, celui-ci doit être utilisé plutôt que la suppression. Cependant, une fois que vous décidez de supprimer un certain nombre d'enregistrements, ils doivent être supprimés à l'aide du logiciel approprié. Par exemple, votre système de centre de services fournira une fonction pour supprimer les enregistrements d'incidents de sécurité.

Si de tels enregistrements sont conservés sur du matériel qui doit être éliminé, tous les disques durs doivent être détruits par un entrepreneur agréé.

Les copies papier des documents qui doivent être éliminés doivent être déchiquetées conformément aux *procédures de gestion des actifs convenues* .