[Logo de l'organisation]

[Nom de l'organisation]

Commented [AES1]: Remplissez tous les champs entre crochets [ ] dans ce document.

PROCEDURES DE SECURITE POUR LE SERVICE DES TECHNOLOGIES DE L'INFORMATION

Commented [AES2]: Certaines parties de ce document, qui doivent être précisées, peuvent constituer des documents distincts (politiques / procédures).

Code :	
Version :	
Date de la version :	
Créé par :	
Approuvée par :	
Niveau de confidentialité :	

Commented [AES3]: Le système de codage des documents doit être aligné avec le système existant de l'organisation pour la codification des documents ; au cas où un tel système n'est pas en place, cette ligne peut être supprimée.

Historique des modifications

Date	Version	Créé par	Description de la modification
	0.1	Advisera	Structure documentaire de base

Table des matières

1. But, domaine d'application et utilisateurs

Ce document a pour but d'assurer un fonctionnement correct et sécurisé des technologies de l'information et de la communication.

Ce document s'applique à l'ensemble du domaine d'application du Système de management de la sécurité de l'information (SMSI), c'est-à-dire à toutes les technologies de l'information et de la communication, ainsi qu'à toute la documentation relative au domaine d'application.

Les utilisateurs de ce document sont les employés de [unité organisationnelle pour les technologies de l'information et de la communication].

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31 et A.8.32
- Politique de sécurité de l'information
- [Plan de reprise en cas de désastre]
- [Politique relative aux appareils mobiles, au télétravail et au travail à distance]
- [Politique de classification des informations]
- [Inventaire des actifs]
- [Politique de sécurité des fournisseurs]
- [Politique de développement sécurisé]
- [Politique de contrôle d'accès]

Commented [AES4]: Vous pouvez consulter un modèle pour ce document dans le dossier "05_Politiques_generales" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES5]: Vous pouvez consulter des modèles pour ces documents dans le dossier "09_Annexe_A_Mesures_de_securite" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

3. Procédures opérationnelles pour les technologies de l'information et de la communication

3.1. Gestion du changement

Chaque changement, apporté aux systèmes opérationnels ou de production, doit être réalisé de la manière suivante :

1. le changement peut être proposé par [préciser les fonctions du poste]
2. le changement doit être autorisé par [titre du poste], qui doit évaluer sa justification concernant l'activité et les conséquences éventuellement négatives sur la sécurité
3. le changement doit être mis en œuvre par [titre du poste]
4. [titre du poste] est chargé de vérifier que le changement a été mis en œuvre conformément aux exigences
5. [titre du poste] est chargé de tester et de vérifier la stabilité du système – le système ne doit pas être mis en production avant qu'un test approfondi n'ait été mené

Commented [AES6]: Supprimer cette section si la mesure

Commented [AES7]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES8]: Supprimer cette section si la Politique de

Commented [AES9]: Il peut être précisé la nature d'un changement réglementé par ce document : l'installation d'un

6. la mise en œuvre des changements doit être présentée aux personnes suivantes : [énumérer tous les titres de poste nécessaires]
7. [illegible]

Les enregistrements des changements sont conservés [indiquer le nom du formulaire ou décrire une autre méthode d'enregistrement changements].

3.2. Gestion des configurations

[Titre du poste] est chargé de consigner les paramètres de configuration du matériel, des logiciels, des services et des réseaux qui doivent être appliqués, pour assurer un fonctionnement correct et sécurisé, et constituer un point de référence à partir duquel les modifications incorrectes seront évaluées.

3.3. Gestion des capacités

[illegible]

3.4. Protection antivirus

[Nom du logiciel antivirus] doit être installé sur chaque plateforme (par ex. serveurs physiques, virtuels ou Cloud), hébergeant des systèmes d'information gérés par le service informatique, et activer les mises à jour automatiques.

3.5. Sauvegarde

3.5.1. Procédure de sauvegarde

Des copies de sauvegarde doivent être créées pour tous les systèmes identifiés dans la [Stratégie de continuité des activités] et suivant la fréquence définie dans ce document.

[illegible]

3.5.2. Tests des copies de sauvegarde

Les copies de sauvegarde et le processus de leur restauration doivent être testés au moins [une fois tous les trois mois], en mettant en œuvre le processus de restauration des données sur [indiquer le serveur où la restauration des données est réalisée] et en vérifiant que toutes les données ont été récupérées avec succès.

Commented [AES10]: Supprimer cette section si la mesure [illegible]

Commented [AES11]: Supprimer cette section si la mesure [illegible]

Commented [AES12]: Supprimer cette section si la mesure [illegible]

Commented [AES13]: Supprimer cette section si la mesure [illegible]

Commented [AES14]: Pour en savoir plus sur ce sujet, consultez cet article : [illegible]

Commented [AES15]: Supprimer cette section si la Politique de [illegible]

Commented [AES16]: Au cas où un tel document n'existe pas, tous les systèmes nécessitant des sauvegardes doivent être énumérés ici, ainsi que la fréquence des sauvegardes. [illegible]

Commented [AES17]: Ajuster la fréquence conformément à [illegible]

[Titre du poste] est chargé de tester les copies de sauvegarde. Les enregistrements des tests de copies de sauvegarde sont conservés [indiquer la forme de l'enregistrement – sur papier ou sous forme électronique, existe-t-il une forme prescrite, etc.].

3.6. Gestion de la sécurité du réseau

[Titre du poste] est responsable de la gestion et du contrôle des réseaux informatiques, pour assurer la sécurité de l'information dans les réseaux, prévenir la fuite des données et protéger les services connectés aux réseaux contre l'accès non-autorisé. Il est donc nécessaire :

- de distinguer la responsabilité opérationnelle relative aux réseaux de la responsabilité relative aux applications sensibles et aux autres systèmes
- de protéger les données sensibles transitant sur le réseau public en [décrire la technologie de protection utilisée et préciser les responsabilités et les personnes responsables]
- de protéger les données sensibles transitant sur des réseaux sans fil en [décrire la technologie de protection utilisée et préciser les responsabilités et les personnes responsables]
- de protéger les équipements connectés au réseau depuis des sites distants en [décrire la technologie de protection utilisée et préciser les responsabilités et les personnes responsables]
- de cloisonner le réseau en [décrire les parties du réseau qui sont cloisonnées - indiquer si le cloisonnement est physique ou logique]
- de séparer les environnements des systèmes de développement, de test et d'exploitation
- de cloisonner le trafic venant d'appareils mobiles, de mettre en place des politiques de pare-feu uniques, des routes statiques, des réseaux locaux virtuels (VLAN), etc.
- d'assurer l'accessibilité des services de réseau en [décrire les mesures qui assurement cet accès]
- de filtrer l'accès aux sites internet qui peuvent présenter des contenus malveillants ou illégaux, ou qui peuvent être utilisés pour la fuite des données
- d'assurer que les horloges système, sur tous les ordinateurs, sont synchronisées [décrire la façon dont elles sont synchronisées et la source de temps précise]

[Titre du poste] doit régulièrement contrôler et tester les mesures mises en œuvre.

3.7. Services de réseau

[Titre du poste] doit définir les caractéristiques de sécurité et le niveau de services attendus pour tous les services de réseau, que ces services soient fournis en interne ou externalisés – ces exigences doivent être consignées auprès des fournisseurs de services.

Si les services de réseau sont externalisés, alors les exigences doivent être précisées dans l'accord conformément à la [Politique de sécurité des fournisseurs].

3.8. Suppression des données

Commented [AES18]: Supprimer cette section si la mesure A.8.20 est jugée inapplicable dans la Déclaration d'applicabilité.

Commented [AES19]: Pour en savoir plus sur ce sujet, consultez ces articles :

• How to manage network security according to ISO 27001 A.13.1
https://advisera.com/27001academy/blog/2016/06/27/how-to-manage-network-security-according-to-iso-27001-a-13-1/

• Requirements to implement network segregation according to ISO 27001 control A.13.1.3
https://advisera.com/27001academy/blog/2015/11/02/requirements-to-implement-network-segregation-according-to-iso-27001-control-a-13-1-3/

Commented [AES20]: Ou se référer à la Politique relative aux

Commented [AES21]: La fréquence doit être précisée -

Commented [AES22]: Les mesures doivent être précisées -

Commented [AES23]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES24]: Supprimer cette section si la mesure

Toutes les données conservées dans les applications, les bases de données, les serveurs et les réseaux doivent être supprimées par le propriétaire de l'actif, lorsqu'elles ne sont plus nécessaires.

Les données doivent être supprimées [décrire la technologie utilisée pour supprimer les données des applications et des équipements].

3.9. Elimination et destruction des équipements et des supports

Toutes les données et les logiciels sous licence conservés sur des supports de stockage mobiles (par ex. sur CD, DVD, clé USB, carte mémoire, mais aussi sur papier) et sur tous les équipements contenant des supports de stockage (par ex. ordinateurs, téléphones mobiles, etc.) doivent être effacés ou leurs supports détruits avant qu'ils ne soient éliminés ou réutilisés.

La personne chargée d'effacer les données / de détruire les supports doit informer le propriétaire des actifs en question, concernant l'effacement / la destruction des données, pour qu'il puisse mettre à jour l'inventaire des actifs.

3.9.1. *Equipements*

[Titre du poste] est responsable de la vérification et de l'effacement des données des équipements, à moins que la Politique de classification des informations n'en dispose autrement. Les données doivent être effacées [décrire la technologie utilisée pour effacer les données des supports des équipements], mais si la sécurité du processus n'est pas suffisante considérant la sensibilité des données, alors le support de stockage doit être détruit.

3.9.2. *Supports de stockage mobiles*

[Titre du poste] est chargé d'effacer les données des supports de stockage mobiles, à moins que la Politique de classification des informations n'en dispose autrement. Les données doivent être effacées [décrire la technologie utilisée pour effacer les données des supports], mais si la sécurité du processus n'est pas suffisante considérant la sensibilité des données, alors le support de stockage doit être détruit.

3.9.3. *Supports papier*

Les employés de l'organisation, manipulant des documents individuels, sont responsables de la destruction des documents papier, à moins que la Politique de classification des informations n'en dispose autrement. Les documents papier sont détruits [au moyen de déchiqueteuses à papier].

3.9.4. *Enregistrements d'effacement et de destruction ; commission de destruction des données*

Les enregistrements d'effacement / de destruction doivent être conservés pour toutes les données portant la mention "Restreint" et "Confidentiel". Les enregistrements doivent inclure les renseignements suivants : informations concernant les supports, date d'effacement / de destruction, méthode d'effacement / de destruction, personne qui a mené à bien l'opération.

Commented [AES25]: Par ex. énumérer les outils spécialisés qui

Commented [AES26]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES27]: Supprimer cette section si la Politique

Commented [AES28]: Supprimer cette section si les mesures

Commented [AES29]: Il peut être en outre précisé que cela

Commented [AES30]: Il peut en outre être précisé que cela

Commented [AES31]: Supprimer cet élément si la mesure A.5.9

Commented [AES32]: Supprimer cette section si la mesure

Commented [AES33]: Doit être supprimé si une telle Politique n'existe pas.

Commented [AES34]: Par ex. la liste des outils spécialisés qui

Commented [AES35]: Par ex. le disque dur d'un serveur.

Commented [AES36]: Supprimer cette section si la mesure

Commented [AES37]: Doit être supprimé si une telle Politique n'existe pas.

Commented [AES38]: Supprimer cette section si la mesure

Commented [AES39]: Doit être supprimé si une telle Politique n'existe pas.

Commented [AES40]: Ou indiquer une autre technologie.

Commented [AES41]: Adapter aux niveaux de confidentialité

Toutes les informations portant la mention "Confidentiel" doivent être effacées / détruites en présence d'une commission composée de personnes autorisées à accéder aux informations en question.

3.10. Transfert des informations

Commented [AES42]: Supprimer cette section si la Politique de [illegible]

3.10.1. Canaux de communication électronique

Les informations de l'organisation peuvent être échangées au travers des canaux de communication électronique suivants : messagerie, téléchargement de fichiers depuis Internet, transfert de données via [fournir les noms des systèmes de communication spécialisés], téléphones, télécopieurs, messages SMS, supports mobiles, et forums et réseaux sociaux.

Commented [AES43]: Le support en question peut être précisé.

Commented [AES44]: Ajouter ou supprimer les canaux de [illegible]

Commented [AES45]: Les forums et réseaux sociaux en [illegible]

[illegible]

Commented [AES46]: Ce texte peut être remplacé en indiquant [illegible]

[illegible]

Commented [AES47]: Doit être supprimé si une telle Politique n'existe pas.

3.10.2. Relations avec les tiers

Les tiers désignent les différents fournisseurs de services, les entreprises pour la maintenance des matériels et des logiciels, les entreprises qui gèrent les transactions ou le traitement des données, les clients, etc.

[Titre du poste] doit élaborer et signer un accord avec le tiers avant d'échanger des informations et / ou des logiciels, verbalement, par des moyens électroniques ou physiques. L'accord peut être sous forme papier ou électronique (par ex. en acceptant les conditions générales) et doit contenir des clauses conformes à l'évaluation des risques, incluant au moins :

- la méthode d'identification de l'autre partie
- les autorisations d'accès à l'information
- le respect de la non-répudiation
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

3.11. Gestion du code source

Commented [AES48]: Supprimer cette section si la mesure [illegible]

Les codes source du programme sont conservés [décrire la mise en œuvre technique] et leur accès est défini dans la [Politique de contrôle d'accès].

Commented [AES49]: Par ex. en utilisant GitHub, Bitbucket, [illegible]

3.12. Utilisation des programmes utilitaires

[Titre du poste] est chargé d'approuver les demandes d'utilisation des programmes utilitaires à privilèges.

3.13. Contrôle des systèmes

En se fondant sur les résultats de l'évaluation des risques, [titre du poste] détermine les journaux qui seront conservés, les systèmes sur lesquels ils seront conservés, la nature de ces systèmes et la durée de leur conservation. Les journaux doivent être conservés pour tous les administrateurs et opérateurs de systèmes sensibles.

[Titre du poste] est chargé, au quotidien, de contrôler les journaux relatifs aux erreurs automatiquement signalées, ainsi que d'inscrire les erreurs signalées par les utilisateurs, d'analyser les raisons pour lesquelles les erreurs se sont produites, d'identifier de nouvelles menaces potentielles, ainsi que les éventuelles fuites de données, et de prendre les mesures correctives appropriées. [Des autorisations spécifiques peuvent être précisées pour des actions dans le cas d'une erreur, ainsi que la façon dont les enregistrements d'erreurs sont conservés.]

[Titre du poste] est chargé d'examiner régulièrement les journaux afin de contrôler les activités des utilisateurs, des administrateurs et des opérateurs système, pour identifier de nouvelles menaces potentielles, ainsi que les éventuelles fuites de données. L'examen est réalisé à intervalles définis par [titre du poste], qui détermine et sélectionne les enregistrements à examiner, et la manière dont l'examen doit en assurer sans enregistré. [Titre du poste] doit être informé des résultats de l'examen.

[Titre du poste] est chargé de contrôler toutes les vulnérabilités des applications et des autres systèmes, et [titre du poste] doit sélectionner les mesures à prendre au cas où de nouvelles vulnérabilités sont identifiées.

[Titre du poste] est chargé de contrôler les configurations, appliquées sur les appareils et les systèmes, par rapport aux configurations approuvées et consignées, et [titre du poste] doit sélectionner les mesures à prendre au cas où les configurations actuelles sont différentes de celles approuvées.

[Titre du poste] est chargé de vérifier les rapports relatifs aux tests d'intrusion et aux évaluations de vulnérabilités réalisés, et de prendre les mesures correctives appropriées.

3.14. Contrôle des menaces extérieures

[Titre du poste] est chargé de contrôler les fournisseurs, les fabricants et les groupes de référence de sécurité afin d'identifier les menaces extérieures qui peuvent avoir un impact sur les applications et les systèmes, et [titre du poste] doit sélectionner les mesures à prendre au cas où de nouvelles menaces sont identifiées.

4. Gestion des enregistrements conservés sur la base de ce document

Commented [AES50]: Supprimer cette section si la mesure

Commented [AES51]: Un programme utilitaire à privilèges est une application capable de modifier ou de contourner les configurations de sécurité (par ex. permet à l'utilisateur de désactiver les caractéristiques de sécurité ou d'accéder à un fichier pour lequel il n'a pas d'autorisation).

Commented [AES52]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES53]: Les journaux peuvent inclure les activités

Commented [AES54]: Supprimer ce paragraphe si la mesure

Commented [AES55]: Supprimer cet élément si la mesure A.5.7

Commented [AES56]: Supprimer cet élément si la mesure

Commented [AES57]: Supprimer ce paragraphe si la mesure

Commented [AES58]: Il peut être précisé que cela inclut par ex.

Commented [AES59]: Supprimer cet élément si la mesure A.5.7

Commented [AES60]: Supprimer cet élément si la mesure

Commented [AES61]: Si nécessaire, préciser la nature de

Commented [AES62]: Supprimer ce paragraphe si la mesure

Commented [AES63]: Supprimer ce paragraphe si la mesure

Commented [AES64]: Supprimer ce paragraphe si la mesure

Commented [AES65]: Supprimer ce paragraphe si la mesure

Commented [AES66]: Supprimer cette section si la mesure

[illegible]	[illegible]	*Personne responsable de la conservation*	*Mesures pour la protection des enregistrements*	[illegible]
[illegible]	[illegible]	[titre du poste]	Une fois créé, l'enregistrement ne peut pas être modifié ultérieurement.	[illegible]
[illegible]	[illegible]	[titre du poste]	Une fois créé, l'enregistrement ne peut pas être modifié ultérieurement.	[illegible]
[illegible]	[illegible]	[titre du poste]	Les journaux sont accessibles en lecture seule ; ils ne peuvent pas être supprimés ou modifiés.	[illegible]
[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] a le droit d'accéder à de tels enregistrements.	[illegible]
[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] a le droit d'accéder à de tels enregistrements.	[illegible]
[illegible]	[illegible]	[titre du poste]	L'armoire est verrouillée ; les clés sont conservées par [fonctions du poste].	[illegible]

Commented [AES67]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation. [illegible]

Commented [AES68]: Adaptez la durée dans cette colonne à [illegible]

[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] a le droit d'accéder à de tels enregistrements.	[illegible]

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

[illegible]

Commented [AES69]: Il ne s'agit que d'une recommandation ; [illegible]

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre d'incidents liés à la sécurité du fonctionnement des systèmes TIC
- [illegible]

[titre du poste]
[nom]

[signature]

Commented [AES70]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.