[Logo de l'organisation]

[Nom de l'organisation]

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

POLITIQUE DE SECURITE DES TECHNOLOGIES DE L'INFORMATION

Commented [AES2]: Pour en savoir plus sur la structure de ce document, consultez cet article :

How to structure the documents for ISO 27001 Annex A controls https://advisera.com/27001academy/blog/2014/11/03/how-to-structure-the-documents-for-iso-27001-annex-a-controls/

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.

Historiques 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 de définir des règles claires pour l'utilisation acceptable du système d'information et des autres actifs informationnels au sein de [nom de l'organisation].

Commented [AES4]: Indiquez le nom de votre organisation.

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 tous les systèmes d'information et tous les autres actifs informationnels utilisés dans le domaine d'application du SMSI.

Les utilisateurs de ce document sont l'ensemble des employés de [nom de l'organisation].

Commented [AES5]: Indiquez le nom de votre organisation.

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19 et A.8.23
- Politique de sécurité de l'information
- [Politique de classification des informations]
- [Procédure de gestion des incidents]
- [Inventaire des actifs]
- [Procédures de sécurité pour le service des technologies de l'information]
- [Politique de transfert des informations]

Commented [AES6]: 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 [AES7]: 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. Utilisation acceptable des actifs informationnels

Commented [AES8]: La mesure dans laquelle il est nécessaire d'appliquer les éléments énumérés doit être fondée sur les résultats de l'évaluation des risques.

3.1. Définitions

Le système d'information – inclut tous les serveurs et les clients, l'infrastructure réseau, les logiciels système et d'application, les données et les autres sous-systèmes et composants appartenant à l'organisation, utilisés par elle ou relevant de sa responsabilité. L'utilisation d'un système d'information comprend également l'utilisation de tous les services internes ou externes, tels que l'accès internet, les e-mails, etc.

3.2. Utilisation acceptable

Les actifs informationnels ne peuvent être utilisés que pour les besoins de l'activité afin d'exécuter des tâches liées à l'organisation.

3.3. Responsabilité des actifs

Commented [AES9]: Supprimer cette section si la mesure A.5.9

Un propriétaire est désigné pour chaque actif informationnel dans l'Inventaire des actifs. Le propriétaire de l'actif est responsable de la confidentialité, de l'intégrité et de la disponibilité de l'information sur l'actif en question.

3.4. Suppression des informations

Lorsqu'elles ne sont plus nécessaires, le propriétaire de l'actif doit supprimer les informations sensibles conservées sur son ordinateur ou appareil mobile.

3.5. Activités prohibées

Il est interdit d'utiliser les actifs informationnels d'une manière qui absorbe inutilement les moyens, qui affaiblit la performance du système d'information ou qui constitue une menace pour la sécurité. Il est également interdit :

- de télécharger des fichiers image ou vidéo qui n'ont pas un objectif commercial, d'envoyer une chaîne de lettres par e-mail, de jouer à des jeux, etc.
- d'installer des logiciels sur un ordinateur local sans l'autorisation expresse de [titre du poste]
- d'utiliser des applications sous, des contrôles ActiveX et autres codes mobiles, sauf en cas d'autorisation de [titre du poste]
- d'utiliser des outils cryptographiques (encryptage) sur un ordinateur local, sauf dans les cas prévus par la Politique de classification des informations
- de télécharger des codes de programme à partir de supports externes
- d'installer ou d'utiliser des périphériques, tels que des modems, des cartes mémoire ou autres dispositifs de stockage et de lecture de données (par ex. des clés USB) sans l'autorisation expresse de [titre du poste]. L'utilisation conforme à la Politique de classification des informations est autorisée.

3.6. Emporter des actifs hors site

Des équipements, des informations ou des logiciels, quelle que soit leur forme ou leur support de stockage, ne peuvent être emportés hors site sans autorisation écrite préalable de [titre du poste].

Tant que lesdits actifs sont hors de l'organisation, ils doivent être contrôlés par la personne qui a obtenu la permission de leur retrait.

3.7. Retour des actifs à la résiliation du contrat

Lors de la résiliation d'un contrat de travail ou d'un autre contrat en vertu duquel divers équipements, logiciels ou informations sous forme électronique ou papier sont utilisés, l'utilisateur doit retourner de tels actifs informationnels à [titre du poste].

3.8. Procédure de sauvegarde

L'utilisateur doit [préciser la méthode de procédure de sauvegarde] toutes les informations sensibles conservées sur son ordinateur au moins une fois par jour.

3.9. Protection antivirus et contre les logiciels malveillants

Commented [AES10]: Supprimer cette section si la mesure

Commented [AES11]: A supprimer si la mesure A.8.19 est jugée

Commented [AES12]: A supprimer si une telle Politique n'existe pas.

Commented [AES13]: Supprimer cette section si la mesure

Commented [AES14]: Il peut être précisé si une telle autorisation s'applique une seule fois ou à long terme et, s'il doit y

Commented [AES15]: Supprimer cette section si la mesure

Commented [AES16]: Supprimer cette section si la mesure

Commented [AES17]: Adaptez la fréquence en fonction des

Commented [AES18]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES19]: Assurez-vous que cela n'interfère pas

Commented [AES20]: Supprimer cette section si la mesure

[Nom du logiciel antivirus] doit être installé sur chaque ordinateur et les mises à jour automatiques doivent être activées.

3.10. Autorisations pour l'utilisation des systèmes d'information

Les utilisateurs du système d'information peuvent accéder uniquement aux actifs du système d'information pour lesquelles ils ont été expressément autorisés par le propriétaire des actifs.

[illegible]

[illegible]

3.11. Responsabilités du compte utilisateur

L'utilisateur ne doit pas, directement ou indirectement, permettre à une autre personne d'utiliser ses droits d'accès, c'est-à-dire le nom d'utilisateur, et ne doit pas utiliser le nom d'utilisateur et / ou le mot de passe d'une autre personne. L'utilisation de noms d'utilisateurs de groupe est interdite.

Commented [AES21]: A supprimer si la mesure A.8.17 est jugée [illegible]

[illegible]

3.12. Responsabilités relatives au mot de passe

Commented [AES22]: Supprimer cette section si la Politique [illegible]

Commented [AES23]: Supprimer cette section si la mesure [illegible]

Les utilisateurs doivent appliquer ces bonnes pratiques de sécurité lors de la sélection et de l'utilisation des mots de passe :

- les mots de passe ne doivent pas être divulgués à d'autres personnes, y compris aux administrateurs système et à l'encadrement
- [illegible]
- [illegible]
- [illegible]
- les mots de passe fiables doivent être sélectionnés de la façon suivante :
  - en utilisant au moins 16 caractères
  - en utilisant au moins un caractère numérique
  - en utilisant au moins une lettre majuscule et au moins une lettre minuscule
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]

- les mots de passe doivent être modifiés tous les 3 mois
- le mot de passe doit être modifié lors de la première connexion au système
- [illegible]
- [illegible]

3.13. Politique du bureau propre et de l'écran vide

Toutes les informations portant la mention "Utilisation interne," "Restreint" ou "Confidentiel", telle que précisée dans la [Politique de classification des informations], sont jugées sensibles dans cette section.

3.13.1. Politique du bureau propre

Si la personne autorisée n'est pas à son poste de travail, tous les documents papier, ainsi que les appareils mobiles (terminaux) et les supports de stockage de données jugés sensibles, doivent être retirés du bureau ou d'autres lieux (imprimantes, télécopieurs, photocopieurs, etc.) pour prévenir l'accès non autorisé.

[illegible]

3.13.2. Politique de l'écran vide

Si la personne autorisée n'est pas à son poste de travail, toutes les informations sensibles doivent être retirées de l'écran et l'accès doit être refusé à tous les systèmes pour lesquels la personne dispose d'une autorisation.

[illegible]

Les informations sur les tableaux blancs (par ex. ceux disponibles dans les salles de réunion) doivent être effacées si elles ne sont plus nécessaires.

3.13.3. Protection des installations et des équipements partagés

Les documents contenant des informations sensibles doivent immédiatement être retirés des imprimantes, télécopieurs et photocopieurs.

Commented [AES24]: Pour en savoir plus sur ce sujet, consultez cet article :

[illegible]

Commented [AES25]: Supprimer cette section si la mesure [illegible]

Commented [AES26]: Supprimer cet élément si les mesures [illegible]

Commented [AES27]: Remplacer par "Procédures de sécurité [illegible]

Commented [AES28]: Supprimer cette section si la mesure [illegible]

Commented [AES29]: Adapter au système utilisé dans l'organisation.

Commented [AES30]: Supprimer cette section si la mesure [illegible]

Les installations pour l'envoi et la réception du courrier [préciser les installations et leurs emplacements] sont protégés par [préciser le mode de protection lorsque la personne autorisée est absente].

Les télécopieurs partagés [préciser les machines et leurs emplacements] sont protégés par [préciser le mode de protection lorsque la personne autorisée est absente].

L'utilisation non autorisée des imprimantes, photocopieurs, scanners et autres équipements partagés pour la copie [préciser les machines et leurs emplacements] est empêchée par [préciser comment].

Avant de quitter les installations pendant une durée plus longue, ou de façon permanente, une inspection détaillée des salles, des bureaux, et des meubles qui s'y trouvent, doit être réalisée pour s'assurer qu'aucun actif de [nom de l'organisation] n'est abandonné.

Commented [AES31]: Par ex. fermeture des installations, etc.

Commented [AES32]: Par ex. fermeture des installations, etc.

Commented [AES33]: Par ex. fermeture des installations,

Commented [AES34]: Par ex. plus de deux semaines.

Commented [AES35]: Indiquez le nom de votre organisation.

3.14. Utilisation d'internet

Internet est accessible uniquement via le réseau local de l'organisation avec une infrastructure appropriée et une protection pare-feu. L'accès direct à Internet via des modems, l'internet mobile, les réseaux sans fil, ou d'autres dispositifs pour l'accès direct à Internet, est interdit.

[Titre du poste] peut bloquer l'accès à certaines pages Internet pour des utilisateurs individuels, des groupes d'utilisateurs ou tous les employés de l'organisation, afin de réduire le risque d'accès à des sites Internet proposant du contenu inadéquat ou illégal, ou qui peuvent être utilisés pour la fuite de données. Si l'accès à certaines pages Internet est bloqué, l'utilisateur peut soumettre une demande écrite à [titre du poste] pour obtenir l'autorisation d'accéder à ces pages. L'utilisateur ne doit pas essayer de contourner de telles restrictions de façon autonome.

L'utilisateur doit considérer les informations reçues par le biais des sites Internet non vérifiés comme peu fiables. Ces informations peuvent être utilisées à des fins commerciales uniquement après vérification de leur authenticité et de leur exactitude.

L'utilisateur est responsable de toutes les conséquences éventuelles résultant de l'utilisation non autorisée ou inappropriée des services Internet ou de leur contenu.

3.15. E-mail et autres méthodes d'échange de messages

Commented [AES36]: Supprimer cette section si la mesure

Les méthodes d'échange de messages, autres que le courrier électronique, comprennent également le téléchargement de fichiers depuis Internet, le transfert de données via [fournir les noms des systèmes de communication spécialisés], les téléphones, les télécopieurs, l'envoi de messages SMS, les supports mobiles, les forums et les réseaux sociaux.

Conformément aux [Procédures de sécurité pour le service des technologies de l'information / Politique de transfert des informations], ainsi qu'à la [Politique de classification des informations], [titre du poste] détermine le canal de communication qui peut être utilisé pour chaque type de données, ainsi que les restrictions éventuelles concernant les personnes autorisées à utiliser les canaux de communication, c'est-à-dire qu'il définit les activités interdites.

Commented [AES37]: Les supports en question doivent être précisés.

Commented [AES38]: Les forums et les réseaux sociaux en

Les utilisateurs ne peuvent envoyer que des messages contenant des informations exactes. Il est interdit d'envoyer des documents proposant un contenu troublant, désagréable, sexuellement explicite, grossier, diffamatoire ou tout autre contenu inacceptable ou illégal. Les utilisateurs ne doivent pas envoyer de messages de spam à des personnes avec lesquelles aucune relation commerciale n'a été établie ou à des personnes qui n'exigeaient pas de telles informations.

Si un utilisateur reçoit un courrier indésirable, il / elle doit en informer [titre du poste].

Lors de l'envoi d'un message à caractère confidentiel, l'utilisateur doit le protéger conformément à la Politique de classification des informations.

L'utilisateur doit enregistrer chaque message contenant des données essentielles pour les activités de l'organisation à l'aide de la méthode indiquée par [titre du poste].

Chaque message électronique doit contenir un avertissement, à l'exception des messages envoyés via des systèmes de communication déterminés par [titre du poste]. Si un utilisateur doit publier un message sur un système d'échange de messages (réseaux sociaux, forums, etc.), il / elle doit clairement indiquer qu'il ne représente pas le point de vue de l'organisation.

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

3.16. Droit d'auteur

Commented [AES40]: Supprimer cette section si la mesure

Les utilisateurs ne doivent pas réaliser des copies non autorisées de logiciels appartenant à l'organisation, sauf dans les cas prévus par la loi, par le propriétaire ou par [titre du poste].

Les utilisateurs ne doivent copier aucun logiciel ni aucun autre contenu original, provenant d'autres sources, et sont responsables de toutes les conséquences qui pourraient en résulter, en vertu du droit de la propriété intellectuelle.

3.17. Informatique mobile

Commented [AES41]: Supprimer cette section si la Politique

Commented [AES42]: Supprimer cette section si la mesure

3.17.1. Introduction

Les équipements d'informatique mobile comprennent toutes sortes d'ordinateurs portables, de téléphones portables, de smartphones, de cartes mémoire et d'autres équipements mobiles utilisés pour la conservation, le traitement et le transfert de données, peu importe le lieu d'utilisation de ces équipements.

Les équipements précités peuvent être emportés hors des locaux seulement après en avoir obtenu l'autorisation, conformément à la section 3.6 – Emporter des actifs hors site de la présente Politique.

3.17.2. Règles fondamentales

Des précautions particulières doivent être prises lorsque l'équipement d'informatique mobile est placé dans des véhicules (y compris les voitures), des espaces publics, des chambres d'hôtel, des espaces de rencontre, des centres de conférence et d'autres zones non-protégées à l'extérieur des locaux de l'organisation.

La personne qui emporte un équipement d'informatique mobile hors des locaux doit suivre les règles suivantes :

- les équipements d'informatique mobile contenant des informations importantes, sensibles ou essentielles ne doivent pas être laissés sans surveillance et doivent être, si possible, physiquement enfermés ou sécurisés à l'aide de serrures spéciales
- lorsqu'un équipement d'informatique mobile est utilisé dans des espaces publiques, l'utilisateur doit s'assurer que les données ne peuvent pas être lues par des personnes non-autorisées
- les mises à jours des correctifs et des autres paramètres du système sont accomplies par [indiquer la manière dont cela est techniquement mis en œuvre ou mentionner un document définissant le processus]
- la protection contre les codes malveillants est installée et mise à jour [indiquer la manière dont cela est techniquement mis en œuvre ou mentionner un document définissant le processus]
- [illegible]

[illegible]

3.18. Télétravail et travail à distance

3.18.1. Introduction

Le télétravail signifie que les équipements d'information et de communication sont utilisés pour permettre aux employés d'effectuer leur travail à l'extérieur de l'organisation, y compris chez eux. Le télétravail ne comprend pas l'utilisation des téléphones mobiles à l'extérieur des locaux de l'organisation.

[illegible]

3.18.2. Règles supplémentaires pour le télétravail

Toutes les personnes en télétravail doivent respecter les règles pour l'informatique mobile, définies à la section 3.17 de ce document, et les règles définies ci-dessous :

Commented [AES43]: Par ex. évaluation hebdomadaire du [illegible]

Commented [AES44]: Par ex. en exécutant l'installation de l'outil pour la protection contre les logiciels malveillants et la [illegible]

Commented [AES45]: Par ex. en accédant au réseau de [illegible]

Commented [AES46]: Par ex. en établissant un canal de [illegible]

Commented [AES47]: Indiquez le type d'informations stocké sur les ordinateurs portables qui pourrait être crypté, conformément aux pratiques de votre organisation.

[illegible]

Commented [AES48]: Par ex. à travers le cryptage du disque [illegible]

Commented [AES49]: Si votre organisation ne dispose pas d'une Politique de classification des informations, remplacez-la par [illegible]

Commented [AES50]: Doit être supprimé si les employés ne [illegible]

Commented [AES51]: Si votre organisation ne dispose pas [illegible]

Commented [AES52]: Vous pouvez utiliser le Programme de sensibilisation à la sécurité suivant pour former vos employés : [illegible]

Commented [AES53]: Pour en savoir plus sur ce sujet, consultez cet article :

[illegible]

Commented [AES54]: Supprimer cette section si la mesure [illegible]

Commented [AES55]: Supprimer cette section si la Politique [illegible]

Commented [AES56]: L'autorisation peut être obtenue sous [illegible]

- l'emplacement physique où est réalisé le télétravail doit être protégé par [indiquer la manière dont cela est techniquement mis en œuvre ou mentionner un document définissant le processus]
- les personnes en télétravail doivent posséder au minimum [énumérer ici les paramètres minimum requis pour le télétravail]
- la prévention de l'accès non-autorisé, des personnes habitant ou travaillant dans le lieu où est réalisé l'activité de télétravail, doit être mis en œuvre conformément à la [Politique de contrôle d'accès] et à la [Politique du bureau propre et de l'écran vide]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

3.19. Contrôle de l'utilisation des systèmes d'information et de communication

Toutes les données créées, conservées, envoyées ou reçues via le système d'information ou d'autres systèmes de communication de l'organisation, y compris diverses applications, des e-mails, Internet, les fax, etc., que ce soit personnel ou non, sont considérées comme la propriété de [nom de l'organisation].

[illegible]

[illegible]

3.20. Incidents

Chaque employé, fournisseur ou tierce personne, qui est en contact avec des données et / ou des systèmes de [nom de l'organisation], doit signaler toute faille du système, tout incident ou tout évènement indiquant un éventuel incident, comme précisé dans la Procédure de gestion des incidents.

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

[illegible]	*Lieu de conservation*	*Personne responsable de la conservation*	[illegible]	[illegible]

Commented [AES57]: Exemples d'éléments à utiliser :
- la prévention de l'accès non-autorisé, des résidents, passants, etc., en utilisant des pièces et des bureaux munis de verrous, en ne travaillant pas dans des espaces partagés, en faisant en sorte d'empêcher que des informations soit vues ou entendues par d'autres, etc.
[illegible]

Commented [AES58]: Par ex. alimentation électrique sans [illegible]

Commented [AES59]: Si la Politique du bureau propre et de [illegible]

Commented [AES60]: Si votre organisation ne dispose pas d'une Politique de classification des informations, remplacez-la par [illegible]

Commented [AES61]: Par ex. participer à des réunions avec la [illegible]

Commented [AES62]: Vous pouvez supprimer ce texte s'il [illegible]

Commented [AES63]: Par ex. modifier la configuration sur les [illegible]

Commented [AES64]: Vous pouvez supprimer ce texte s'il [illegible]

Commented [AES65]: Indiquez le nom de votre organisation.

Commented [AES66]: Indiquez le nom de votre organisation.

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

[redacted]	[dossier intranet]	[titre du poste]	[redacted]	[redacted]
[redacted]	[dossier intranet]	[titre du poste]	[redacted]	[redacted]
[redacted]	[dossier intranet]	[titre du poste]	[redacted]	[redacted]
[redacted]	[dossier intranet]	[titre du poste]	[redacted]	[redacted]
[redacted]	[dossier intranet]	[titre du poste]	[redacted]	[redacted]
[redacted]	[dossier intranet]	[titre du poste]	[redacted]	[redacted]

Commented [AES68]: Ajuster si nécessaire.

Commented [AES69]: Ajuster si nécessaire.

Commented [AES70]: Ajuster si nécessaire.

Commented [AES71]: Ajuster si nécessaire.

Commented [AES72]: Ajuster si nécessaire.

Commented [AES73]: Ajuster si nécessaire.

Seul [titre du poste] peut accorder à d'autres employés l'accès aux documents mentionnés ci-dessus.

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

Le propriétaire de ce document est [titre du poste], qui doit vérifier et, si nécessaire, mettre à jour le document au moins [one/two/four per] an.

Commented [AES74]: Il ne s'agit que d'une recommandation ; ajuster si nécessaire.

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 l'utilisation inacceptable ou non-autorisée des actifs informationnels
- le nombre d'incidents liés aux programmes de formation et de sensibilisation inappropriés proposés aux employés, concernant l'utilisation des actifs informationnels

[titre du poste]
[nom]

[signature]

Commented [AES75]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.