[Logo de l'organisation]

[Nom de l'organisation]

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

POLITIQUE DE CLASSIFICATION DES INFORMATIONS

Commented [AES2]: Pour apprendre à classifier des informations, consultez cet article :

Information classification according to ISO 27001
https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/

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 la protection des informations à un niveau approprié.

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 types d'informations, indépendamment de leur forme – documents électroniques ou papier, applications et bases de données, connaissances des personnes, etc.

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

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

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.9, A.5.10, A.5.12, A.5.13, A.5.14, A.7.10, A.8.3, A.8.5, A.8.11 et A.8.12
- Politique de sécurité de l'information
- Rapport d'évaluation et de traitement des risques
- Déclaration d'applicabilité
- Inventaire des actifs
- Liste des exigences légales, réglementaires, contractuelles et autres
- Procédure de gestion des incidents
- [Procédures de sécurité pour le service des technologies de l'information] / [Politique d'élimination et de destruction]
- Politique de sécurité des technologies de l'information

Commented [AES5]: 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 [AES6]: Vous pouvez consulter un modèle pour ce document dans le dossier "06_Evaluation_et_traitement_des_risques" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES7]: Vous pouvez consulter un modèle pour ce document dans le dossier "07_Applicabilite_des_mesures" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES8]: Si vous ne disposez pas de cette Liste, alors énumérez dans ces crochets toutes les obligations légales et réglementaires relatives à la classification de l'information.

Commented [AES9]: Sélectionnez le document qui prescrit l'effacement sécurisé des données.

3. Informations classifiées

3.1. Etapes et responsabilités

Les étapes et les responsabilités pour la gestion de l'information sont les suivantes :

Nom de l'étape	[illegible]
1. Saisie de l'actif informationnel dans l'Inventaire des actifs	[illegible]
2. Classification de l'information	[illegible]
3. Marquage de l'information	[illegible]
4. Gestion de l'information	[illegible]

Si des informations classifiées proviennent de sources extérieures à l'organisation, [titre du poste] est responsable de leur classification conformément aux règles prescrites dans cette Politique, et cette personne devient le propriétaire d'un tel actif informationnel.

3.2. Classification des informations

3.2.1. Critères de classification

Le niveau de confidentialité est déterminé en fonction des critères suivants :

- la valeur de l'information, fondée sur les impacts déterminés lors de l'évaluation des risques
- [illegible]
- [illegible]

Commented [AES10]: Inclut également les règles de confidentialité.

3.2.2. Niveaux de confidentialité

Toutes les informations doivent être classifiées par niveaux de confidentialité.

Niveau de confidentialité	[illegible]	[illegible]	***Restriction d'accès***
Public	[illegible]	[illegible]	L'information est accessible au public
Utilisation interne	[illegible]	[illegible]	L'information est accessible à tous les employés et à certains tiers
Restreint	[illegible]	[illegible]	L'information est accessible uniquement à un groupe spécifique d'employés et à des tiers autorisés
Confidentiel	[illegible]	[illegible]	L'information est accessible uniquement à des individus au sein de l'organisation

Commented [AES11]: Les niveaux de confidentialité et le [illegible]

La règle fondamentale consiste à appliquer le niveau de confidentialité le plus bas, permettant d'assurer un niveau de protection adéquat, afin d'éviter des coûts de protection inutiles.

3.2.3. Liste des personnes autorisées

Les informations marquées de la mention "Restreint" et "Confidentiel" doivent être accompagnées d'une Liste des personnes autorisées, dans laquelle le propriétaire de l'information indique les noms et les fonctions des personnes ayant le droit d'accéder à cette information.

La même règle s'applique au niveau de confidentialité "Utilisation interne" si des personnes extérieures à l'organisation ont accès à un tel document.

3.2.4. Reclassification

Les propriétaires d'actifs doivent examiner le niveau de confidentialité de leurs actifs informationnels tous les [deux ans] et déterminer si le niveau de confidentialité peut être modifié. Dans la mesure du possible, le niveau de confidentialité doit être abaissé.

Commented [AES12]: Il ne s'agit que d'une recommandation ; ajuster en fonction du nécessaire.

3.3. Marquage de l'information

Les niveaux de confidentialité doivent être marqués de la façon suivante :

- **documents papier** – le niveau de confidentialité est indiqué dans le coin supérieur droit de chaque page du document ; il est également indiqué sur la couverture, ou sur l'enveloppe contenant un tel document, ainsi que sur le dossier de classement dans lequel le document est conservé
- **documents électroniques** – le niveau de confidentialité est indiqué dans le coin supérieur droit de chaque page du document
- **systèmes d'information** – le niveau de confidentialité, dans les applications et les bases de données, doit être indiqué sur l'écran d'accès au système, ainsi que dans le coin supérieur droit de chaque écran consécutif affichant des informations confidentielles
- **messagerie électronique** – le niveau de confidentialité est indiqué dans la première ligne du corps du message
- **supports de stockage électroniques** (disques, cartes mémoire, etc.) – le niveau de confidentialité doit être indiqué sur la face supérieure d'un tel support
- **informations transmises oralement** – le niveau de confidentialité des informations confidentielles transmises lors de communications individuelles, par téléphone ou par d'autres moyens de communication, doit être communiqué avant l'information elle-même

3.4. Gestion des informations classifiées

Commented [AES13]: Toutes les règles formulées ici être adaptées aux besoins de l'organisation.

Toutes les personnes qui accèdent à des informations classifiées doivent respecter les règles énumérées dans le tableau suivant. [Titre du poste] doit engager une procédure disciplinaire à chaque violation de ces règles ou si l'information est communiquée à des personnes non-autorisées. Chaque incident lié à la gestion des informations classifiées doit être signalé, conformément à la Procédure de gestion des incidents.

Les actifs informationnels peuvent être empruntés à l'extérieur des locaux uniquement après en avoir obtenu l'autorisation conformément à la Politique de sécurité des technologies de l'information.

Commented [AES14]: Supprimer ce paragraphe si la mesure n'est pas applicable.

La méthode pour l'effacement et la destruction sécurisés des supports est énoncée dans le document de [Procédures de sécurité pour le service des technologies de l'information] / [Politique d'élimination et de destruction].

Commented [AES15]: Sélectionnez le document qui prescrit

	Utilisation interne	*Restreint**	*Confidentiel**
Documents papier	• si envoyé à des destinataires extérieurs à l'organisation, le document doit être expédié en recommandé [illegible]	• le document doit être conservé dans une armoire verrouillée [illegible]	• le document doit être conservé dans un coffre-fort [illegible]
Documents électroniques	• l'accès au système d'information où le document est conservé doit être protégé par un mot de passe fiable [illegible]	• l'accès au système d'information où le document est conservé doit être protégé par une authentification à deux facteurs [illegible]	• le document doit être conservé sous une forme cryptée [illegible]

	[illegible]	[illegible]	[illegible]
Systèmes d'information	• l'accès au système d'information doit être protégé par un mot de passe fiable • [illegible] • [illegible]	• l'accès au système d'information doit être protégé par une authentification à deux facteurs • [illegible] • [illegible]	• l'accès au système d'information doit être protégé par une authentification à deux facteurs, à l'aide de cartes à puce de jetons ou de lecteurs biométriques • [illegible] • [illegible]

		[illegible]	
Messagerie électronique	• l'expéditeur doit s'assurer de l'identité destinataire • [illegible]	• les e-mails doivent être cryptés s'ils sont envoyés à des destinataires extérieurs à l'organisation • [illegible] • [illegible]	• tous les e-mails doivent être cryptés • [illegible] • [illegible]
Supports de stockage électronique	• les supports et les dossiers doivent être protégés par un mot de passe • [illegible]	• les supports et les dossiers doivent être cryptés • [illegible]	• les supports et les dossiers doivent être cryptés • [illegible]
Informations transmises oralement	• les personnes non-autorisées ne doivent pas être présente dans la pièce lorsque l'information est communiquée	• la pièce doit être insonorisée • [illegible]	• la pièce doit être insonorisée • [illegible]

			[illegible]

*Des mesures sont implémentées de façon cumulative, c'est-à-dire que les mesures pour tous les niveaux de confidentialité impliquent la mise en œuvre de mesures définies pour des niveaux de confidentialité inférieurs – si des mesures plus strictes sont prescrites pour un niveau de confidentialité plus élevé, alors seules ces mesures sont mises en œuvre.

3.5. Masquage des données

Commented [AES16]: Supprimer cette section si la mesure [illegible]

Si le propriétaire de l'actif considère que l'exposition aux données est une préoccupation (par ex. données personnelles, secrets commerciaux, etc.), l'information doit au moins comporter la mention "RESTREINT" et ces règles supplémentaires doivent être appliquées pour empêcher l'affichage des données :

- Informations sur support papier : les données, non nécessaires à l'utilisateur, doivent être masquées par la suppression ou la dissimulation des données (par ex. en couvrant le texte avec une bande noire).
- [illegible]

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

[illegible]	[illegible]	*Personne responsable de la conservation*	*Mesures pour la protection des enregistrements*	[illegible]
[illegible]	[illegible]	Propriétaire des actifs informationnels	Les mêmes que pour la protection de l'information	[illegible]

Commented [AES17]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation. [illegible]

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

[illegible]

Commented [AES18]: Il ne s'agit que d'une recommandation ; [illegible]

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

- le nombre d'incidents liés à l'accès non autorisé à l'information
- [illegible]

[titre du poste]
[nom]

[signature]

Commented [AES19]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.