[Logo de l'organisation]

[Nom de l'organisation]

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

POLITIQUE DE DEVELOPPEMENT SECURISE

Commented [AES2]: Pour en savoir plus sur ce sujet, consultez cet article :

How to integrate ISO 27001 controls into the system/software development life cycle (SDLC)
https://advisera.com/27001academy/blog/2017/01/24/how-to-integrate-iso-27001-controls-into-the-system-software-development-life-cycle-sdlc/

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 de définir les règles fondamentales relatives au développement sécurisé de logiciels et de systèmes.

Ce document s'applique au développement et à la maintenance de tous les services, architectures, logiciels et systèmes qui font partie du Système de management de la sécurité de l'information (SMSI).

Les utilisateurs de ce document sont tous les employés qui travaillent sur le développement et la maintenance au sein de [nom de l'organisation].

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

2. Documents référencés

- Norme ISO/IEC 27001, clauses A.5.33, A.8.11, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.32 et A.8.33
- Méthodologie d'évaluation et de traitement des risques
- Politique de sécurité des fournisseurs
- [Politique de gestion du changement] / [Procédures de sécurité pour le service des technologies de l'information]
- Plan de formation et de sensibilisation

Commented [AES5]: 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 [AES6]: Choisissez lequel de ces deux documents vous utiliserez.

Commented [AES7]: Vous pouvez consulter un modèle pour ce document dans le dossier "11_Formation_et_sensibilisation" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

3. Développement et maintenance sécurisés

Commented [AES8]: Etant donné que la technologie utilisée

3.1. Evaluation des risques relatifs au processus de développement

En complément de l'évaluation des risques réalisée conformément à la Méthodologie d'évaluation et de traitement des risques, [titre du poste] doit périodiquement procéder à l'évaluation des éléments suivants :

Commented [AES9]: Si nécessaire, indiquez à quelle fréquence.

- les risques liés à l'accès non-autorisé à l'environnement de développement
- les risques liés à des changements non-autorisés de l'environnement de développement
- les vulnérabilités techniques des systèmes informatiques utilisés dans l'organisation
- [illegible]
- [illegible]
- [illegible]

Commented [AES10]: Il ne s'agit que de recommandations ;

3.2. Sécuriser l'environnement de développement

Commented [AES11]: Supprimer cette section si la mesure

[Identifier les exigences internes et externes ; décrire ici la manière dont seront mis en œuvre l'accès à l'environnement de développement limité aux seuls employés autorisés, la séparation de l'environnement de test et de production et les sauvegardes.]

3.3. Principes d'ingénierie des systèmes sécurisés

[Titre du poste] publiera les procédures d'ingénierie des systèmes d'information sécurisés, relatives au développement de nouveaux systèmes et à la maintenance des systèmes existants, ainsi qu'à la définition des normes minimales de sécurité qui doivent être respectées.

[redacted]

3.4. Codage sécurisé

[Titre du poste] publiera les procédures de codage sécurisé des systèmes d'information, relatives au développement de nouveaux systèmes et à la maintenance des systèmes existantes, ainsi qu'à la définition des pratiques minimales de codage sécurisé qui doivent être respectées.

[redacted]

3.5. Exigences de sécurité

Lors de l'acquisition de nouveaux systèmes d'information ou du développement ou de la modification de systèmes existants, [titre du poste] doit consigner les exigences de sécurité dans la Spécification des exigences relatives aux systèmes d'information.

3.6. Exigences de sécurité relatives aux réseaux publics

[Titre du poste] est responsable de la définition des mesures de sécurité relatives à l'information dans les services d'application transitant par les réseaux publics :

- la description des systèmes d'authentification qui doivent être utilisés
- la description de la manière dont la confidentialité et l'intégrité de l'information, ainsi que la protection des données personnelles, doivent être assurées
- [redacted]

[Titre du poste] est responsable de la définition des mesures relatives aux transactions en ligne, qui doit inclure les éléments suivants :

- la manière dont l'acheminement erroné sera empêché
- la manière dont la transmission incomplète de données sera empêchée
- la manière dont la modification non-autorisée d'un message sera empêchée
- [redacted]

3.7. Vérification et test de la mise en œuvre des exigences de sécurité

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

Commented [AES13]: Par ex. des conseils sur les techniques de programmation sécurisée (séparément pour chaque langage de programmation), des techniques d'authentification d'utilisateurs, des contrôles de sessions sécurisées, des validations de données, etc.

Commented [AES14]: Supprimer ce paragraphe si la mesure [redacted]

Commented [AES15]: Supprimer cette section si la mesure [redacted]

Commented [AES16]: Par ex. des conseils sur les techniques de [redacted]

Commented [AES17]: Supprimer ce paragraphe si la mesure [redacted]

Commented [AES18]: Supprimer cette section si la mesure [redacted]

Commented [AES19]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES20]: Autrement, vous pouvez indiquer qu'il [redacted]

Commented [AES21]: Supprimer cette section si la mesure [redacted]

Commented [AES22]: Il ne s'agit que de recommandations ; [redacted]

Commented [AES23]: Les mesures peuvent comprendre les [redacted]

Commented [AES24]: Il ne s'agit que de recommandations ; [redacted]

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

[Titre du poste] est chargé de définir la méthodologie, les responsabilités et le calendrier de vérification du respect de toutes les exigences issues de la Spécification des exigences relatives aux systèmes d'information, et du caractère acceptable du système pour la production.

3.8. Dépôt

[Décrire ici où le code et tous les autres fichiers relatifs au développement sont conservés, et la manière dont ils sont protégés de l'accès et des modifications non autorisés.]

3.9. Contrôle de version

[Définir ici le système de contrôle de version (numérotation, dates, etc.) et la manière dont il est appliqué dans votre environnement de développement.]

3.10. Contrôle des changements

Les changements apportés dans le développement et pendant la maintenance des systèmes doivent être réalisés conformément à la [Politique de gestion du changement] / aux [Procédures de sécurité pour le service des technologies de l'information].

3.11. Protection des données de test

Les données confidentielles, ainsi que les données qui peuvent être liées à des personnes individuelles, ne doivent pas servir de données de test. [Des exceptions peuvent être approuvées uniquement par [titre du poste], auquel cas [titre du poste] doit définir la manière dont ces données de test sont protégées.

3.12. Formation à la sécurité requise

[Titre du poste] définit le niveau de compétences et de connaissances requises en matière de sécurité, pour le processus de développement, et propose les formations à [titre du poste]. [Titre du poste] inscrit des formations appropriées dans le Plan de formation et de sensibilisation.

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

[Nom de l'enregistrement]	[Lieu de conservation]	*Personne responsable de la conservation*	*Mesures pour la protection des enregistrements*	[Temps de rétention]
[Liens des risques relatifs au processus de développement]	[Ordinateur de [titre du poste]]	[titre du poste]	Seul [titre du poste] peut accéder à ces fichiers.	[1 an pour les liens qui ne sont plus valides]
[Procédure pour l'ingénierie des systèmes]	[Intranet de l'organisation]	[titre du poste]	Seul [titre du poste] peut publier et modifier ces fichiers.	[1 an pour les procédures qui ne sont plus

Commented [AES26]: Par ex. les entrées de test et les résultats attendus, les outils d'analyse de codes ou les scanners de vulnérabilité.

Commented [AES27]: La bonne pratique consiste à faire

Commented [AES28]: Non seulement le test final lorsque le

Commented [AES29]: Supprimer cette section si la mesure

Commented [AES30]: Pour en savoir plus sur ce sujet, consultez cet article :

Commented [AES31]: Choisissez lequel de ces deux documents vous utiliserez.

Commented [AES32]: Supprimer cette section si la mesure

Commented [AES33]: Modifiez ces enregistrements pour les faire correspondre aux pratiques de votre organisation.

Commented [AES34]: Adaptez la durée dans cette colonne à

[illegible]	[illegible]	[titre du poste]	Seul [titre du poste] peut publier et modifier ces fichiers.	[illegible]

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

[illegible]

Commented [AES35]: 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 résultant de mesures de sécurité défaillantes intégrées aux systèmes

6. Annexes

- Annexe 1 – Spécification des exigences relatives aux systèmes d'information

[titre du poste]
[nom]

[signature]

Commented [AES36]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.