POLITIQUE DE SECURITE DE L'INFORMATION

Identification du document	
Référence	POL1 [01] – GRADeS971 – PSSI
Date dernière mise à jour	Voir GED du SMSI
Version	**3**
Classification	**Confidentiel**
Propriétaire	GRADeS 971
Destinataires	☒Ensemble du personnel du GRADeS Archipel 971 ☐Bénéficiaires ☐Partenaires ☐Fournisseurs
Nombre de pages	10

Historique des versions

Historique des versions			
Version	**Date**	**Rédaction**	**Modifications**
1.0	08/07/2019	Yves NORMAND	CREATION
	30/11/2015	Anthony FORBIN	FINAL
	26/11/2019	Cédric PRADEL	MAJ pour certification HDS

Rédaction

AUTEURS(S)		
Fonction	**Nom**	**Date**
Consultant	Yves NORMAND	08/07/2019
Voir GED du SMSI		

Approbation

RELECTEUR(S)		
Fonction	**Nom**	**Date**
RSSI	Harris GLADONE	Voir GED SMSI

Validation

VALIDATION		
Fonction	**Nom**	**Date**
Directeur GRADeS 971	Anthony FORBIN	Voir GED SMSI

Sommaire

Le mot du directeur

La sécurité du système d'information est devenue un facteur indispensable au bon fonctionnement des entreprises et notamment gage de qualité des activités du GRADeS.

Ce dernier ayant pour mission de mettre en œuvre et de maintenir les services numériques concourant à l'amélioration de la prise en charge coordonnée des patients du territoire guadeloupéen.

Son système d'information est désormais devenu une composante stratégique. L'utilisation croissante des systèmes d'information en santé induit de fait la nécessité de garantir la fiabilité, la disponibilité, l'intégrité, la confidentialité des données partagées.

Outre l'intérêt apporté par le numérique, il s'accompagne de son lot de risques et de menaces qu'il convient de mesurer et d'appréhender selon les règles de l'art, d'où la nécessité impérieuse pour le GRADeS de s'inscrire pleinement dans le respect des exigences règlementaires et listées au sein des référentiels ISO 27001 et HDS.

Le GRADeS (Groupement Régional d'Aide au Développement de la eSanté) a pour vocation de développer l'ensemble des services numériques concourant à l'amélioration de la prise en charge coordonnées des patients à l'échelle du territoire guadeloupéen.

Il héberge de fait une quantité importante de données de santé à caractère personnelle, ce qui requiert une certification HDS et donc un haut niveau de sécurité pour cette structure incontournable pour le développement de la eSanté territoriale.

1 But, portée et audience

L'objectif de cette politique de haut niveau est de définir le but, la direction, les principes et les règles de base pour le management de la sécurité de l'information.

La Politique est appliquée à l'ensemble du Système de Management de la Sécurité de l'Information (SMSI) tel que défini dans le Document du domaine d'application du SMSI et dans son manuel associé.

Les utilisateurs de ce document sont les employés du GRADeS Archipel 971, ainsi que les tierces parties concernées.

1.1 Documents référencés

Document	Référence / Lien
PSSI MCAS	https://www.legifrance.gouv.fr/jo_pdf.do?cidTexte=JORFTEXT000031386468
Norme ISO/IEC 27001, Clause 4 à 10	Référentiel ISO/IEC 27001
Norme ISO/IEC 27001, Clause 5	Référentiel ISO/IEC 27001
Norme ISO/IEC 27001, A.5	Référentiel ISO/IEC 27001
Norme ISO/IEC 27001, exigences Annexe A	Référentiel ISO/IEC 27001

1.2 Terminologie de base de la sécurité de l'information

La terminologie employée dans ce document est explicitée dans un glossaire centralisé, nommé TRV [03] - GRADeS971 – GLOSSAIRE, disponible dans l'espace documentaire du GRADeS.

2 Principes organisationnels

2.1 Politique de sécurité

2.1.1 Buts et objectifs

Les objectifs généraux du système de management de la sécurité de l'information sont alignés avec ceux métiers de l'organisation tels que :

- Maintenir un haut niveau de professionnalisme au GRADeS;
- Renforcer la confiance des patients et des acteurs de santé ;
- Réduire les dommages causés par des incidents potentiels ;
- Participer au processus de conformité aux exigences liées à la certification d'hébergeur de données de santé de l'organisme ;
- Participer à la démarche conformité aux lois et règlements applicables.

Le directeur du GRADeS est responsable de la revue de ces objectifs généraux du SMSI et d'en déterminer de nouveaux.

Les objectifs pour les mesures individuelles de sécurité ou pour des groupes de mesures sont proposés par le RSSI et le DPO, et validés par le directeur du GRADeS dans la Déclaration d'applicabilité POL1 [08] - GRADeS971 - DECLARATION D'APPLICABILITE (DDA)

Tous les objectifs doivent être révisés au moins une fois par an conformément à sa politique de de gouvernance du SMSI.

Le GRADeS mesure le niveau de satisfaction des bénéficiaires au travers des Assemblés Générales et des actions d'audit internes et autres revues dont le comité SIDP.

2.1.2 Exigences de sécurité de l'information

Cette Politique et l'ensemble du SMSI doivent être en conformité avec les exigences légales et règlementaires applicables à l'organisation dans le domaine de la sécurité de l'information, ainsi qu'avec les obligations contractuelles.

Une liste détaillée de l'ensemble des exigences contractuelles et légales est fournie dans le registre des obligations légales REG [07] - GRADeS971 - REGISTRE DES OBLIGATIONS LÉGALES

2.1.3 Protection du patrimoine informationnel

Le Grades est le propriétaire de ses actifs et est le propriétaire des risques des actifs dont l'inventaire et la classification sont faits dans GLPI. Il en assure la protection afin de réduire les risques à un niveau acceptable. Il s'engage également dans la sécurisation de son environnement en respectant notamment sa politique de sécurité physique et environnementale et en identifiant et en renforçant de façon adaptée les aires les plus sensibles.

2.1.4 Protection de la vie privée

Le GRADeS s'engage à mettre en œuvre l'ensemble des dispositions techniques et organisationnelles nécessaires afin d'assurer la protection de la vie privée conformément à sa politique de protection des données.

Pour cela, il s'appuie sur des dispositions particulières pour assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité des données et des enregistrements associés conformément à ses politiques de gestion des accès

et des habilitations POL2 [06] - GRADeS971 - POLITIQUE DE CONTRÔLE DES ACCÈS et de gestions des traces POL2 [03] - GRADeS971 - POLITIQUE DE GESTION DES TRACES.

Par ailleurs, il s'appuie également sur sa politique de gestion des sauvegardes POL2 [04] - GRADeS971 - POLITIQUE DE SAUVEGARDE pour garantir la disponibilité et la résilience.

2.2 Organisation de la sécurité

2.2.1 Acteurs

Le SMSI du GRADeS s'appuie sur les fonctions de base ci-dessous afin de garantir sa pertinence, sa pérennité et son efficacité le(la) :

- directeur du GRADeS Archipel 971 est responsable de veiller à ce que le SMSI soit implémenté conformément à cette Politique, et d'assurer toutes les ressources nécessaires.
- responsable de la sécurité des systèmes d'information est responsable de la coordination opérationnelle du SMSI, du suivi du plan d'action SSI et de rapporter au sujet de sa performance.
- délégué à la protection des données est le chef d'orchestre de la conformité en matière de protection des données au sein de l'organisme.
- l'assistante de direction est en charge notamment de la réception et de l'envoi des courriers émis ou à destination de l'organisme ainsi que de leur numérisation et du respect de la confidentialité des documents.
- Les responsables des départements ont pour charge d'assurer l'intégrité, de la disponibilité et de la confidentialité des actifs.

2.2.1 Gouvernance

Le GRADeS organise le pilotage et le suivi de son SMSI conformément aux modalités indiquées dans le politique de gouvernance du SMSI GC [01] - GRADeS971 - POLITIQUE DE GOUVERNANCE DU SMSI

2.3 Gestion des risques SSI

La politique de sécurité de l'information du GRADeS est fondée sur la gestion des risques liés à la sécurité de l'information. Il fixe sa méthodologie d'évaluation et de traitement des risques au travers de sa politique de gestion des risques POL1 [04] - GRADeS971 - POLITIQUE DE GESTION DU RISQUE.

Les mesures sélectionnées et leur état d'implémentation sont énumérés dans la Déclaration d'applicabilité POL1 [08] - GRADeS971 - DECLARATION D'APPLICABILITE (DDA)

2.4 Sécurité et cycle de vie

Le GRADeS mesure l'accomplissement de tous les objectifs du SMSI. Le responsable de la sécurité des systèmes d'information est en charge de la définition d'une méthode pour la mesure de l'accomplissement de ces objectifs. Cette mesure devra être réalisée au moins une fois par an. Le RSSI analyse et évalue les résultats de ces mesures afin de les rapporter au directeur du GRADeS lors de la revue de Direction.

Le délégué à la protection des données organise et contrôle le respect des dispositions règlementaire prévues par le RGPD et rapporte chaque année de ses activités au niveau le plus élevé de la direction du GRADeS conformément aux lignes directrices concernant les délégués à la protection des données.

3 Principes de mise en œuvre

3.1 Aspects humains

L'humain est un maillon essentiel dans le processus global visant à garantir la pérennité et l'efficacité du SMSI. Pour cela, le directeur du GRADeS s'assure que chacun connaît ses missions et de l'adéquation des connaissances et des compétences à l'emploi. Il s'assure de la diffusion de la culture et du respect des règles en matière de sécurité de l'information conformément à la Politique SSI appliquée aux ressources humaines.

3.2 Plan de reprise des activités

La gestion des évènements redoutés est réalisée conformément à la politique de gestion des incidents POL1 [03] - GRADeS971 -POLITIQUE DE GESTION DES INCIDENTS en accord avec les plans de reprise des activités notamment pour satisfaire aux objectifs de performance et d'obligations contractuelles. Ces dispositions sont évaluées annuellement pour s'assurer de la pertinence de l'organisation et des moyens mis en œuvre.

3.3 Gestion des tiers et relation avec les autorités compétentes

L'action du GRADeS s'inscrit au service des acteurs de santé des îles de Guadeloupe, Saint-Martin, Saint-Barthélemy ainsi que des départements français d'Amérique. Pour s'assurer de la cohérence de son SMSI, il communique et formalise le dispositif applicable dans le cadre de son SMSI à l'ensemble de ses bénéficiaires. Il les informe également de leurs devoirs et de leurs droits.

Dans le cadre de ses missions, le GRADeS s'appuie sur un ensemble de fournisseurs et partenaires avec lesquels il organise et formalise le respect de ses différentes obligations et de l'intégrité de son SMSI conformément aux chartes prestataires et administrateurs, CT [03] - GRADES971 - CHARTE DES PRESTATAIRES, CT [02] - GRADeS971 - CHARTE DES ADMINISTRATEURS.

Dans le cadre de ses activités, le GRADeS a recours à des autorités compétentes en fonction des domaines d'applicabilité :

- ARS ➔ rôle d'animation de la stratégie du développement de la eSanté sur le territoire et inscrit les priorités du GRADeS dans le cadre d'un CPOM (contrat pluriannuel d'objectifs et de moyens, COPIL eSanté mensuel et CSA financier mensuel)
- Ministère de Santé ➔ au travers de ses services et notamment la DGOS et autres services d'état a pour charge de transmettre les directives et autres instructions qui s'appliquent au champ d'action des GRADeS ou des ARS au travers des différents COPIL
- ANSSI ➔ outre le fait de fixer le cadre sécuritaire, méthodologique et réglementations en matière de sécurité, l'ANSI représente le référent pour la centralisation de la déclaration des incidents en lien avec le stockage des données numériques de santé
- ANS ➔ missionné par l'état pour définir la feuille de route du numérique en santé. L'ANS s'inscrit dans un co-pilotage avec le GRADeS en région (RCR MSS, RCR LABO, Ateliers thématiques, ateliers Convergence, …)

- CNIL ➔ autorité de contrôle pour la protection des données à caractère personnel

3.4 Gestion des incidents

Les incidents liés à la sécurité de l'information font l'objet d'une attention toute particulière. Ils doivent être tous rapportés au responsable de la sécurité des systèmes d'information conformément à la politique de gestion des incidents POL1 [03] - GRADeS971 -POLITIQUE DE GESTION DES INCIDENTS.

Ils devront également être rapportés au délégué à la protection des données dès lors que la violation impacte potentiellement des données à caractère personnel.

3.5 Sensibilisation et formation

Le directeur du GRADeS organise la diffusion de la culture de la sécurité de l'information auprès de l'ensemble de ses collaborateurs.

Chaque année, en collaboration avec le RSSI et le DPO, le responsable du suivi et de la conformité propose au directeur du GRADeS un plan de formation et sensibilisation (CT [04] - GRADeS971 - PLAN DE SENSIBILISATION ET DE FORMATION ANNUEL) au profit du personnel afin de s'assurer de l'adéquation des qualifications et des compétences du personnel aux enjeux du SMSI.

3.6 Communication de la Politique

Le RSSI veille à ce que tous les collaborateurs du GRADeS Archipel 971, ainsi que tous les tiers, soient dûment informé des dispositions prévues par cette politique.

Le GRADeS organise la communication sur son SMSI autour de son plan de communication du SMSI afin de maitriser l'information diffusée en interne et à des tiers.

4 Principes techniques

4.1 Gestion des accès et des habilitations

Le directeur du GRADeS s'assure du respect de la Politique de gestion des accès et des habilitations par l'ensemble des acteurs du SMSI POL2 [06] - GRADeS971 - POLITIQUE DE CONTRÔLE DES ACCÈS.

4.2 Journalisation

La politique de gestion des traces (POL2 [03] - GRADeS971 - POLITIQUE DE GESTION DES TRACES) organise la conservation et le suivi des journaux d'évènement notamment en matière d'intégrité, de stockage, de surveillance, de durée de conservation, d'analyse, de qualification et de traitement.

4.3 Gestion des clés cryptographiques,

La politique de cryptographie (POL2 [07] - GRADeS971 - POLITIQUE DE CRYPTOGRAPHIE) fixe les conditions de gestion et d'utilisation des outils et des algorithmes de chiffrement au sein de l'organisme.

5 Validité et gestion documentaire

La date de validité du document est celle de sa **publication au sein de l'espace documentaire** partagé du GRADeS.

Le présent document sera automatiquement soumis à une **revue annuelle** grâce aux fonctionnalités de la GED de l'entreprise.

Le propriétaire de ce document est le directeur du département technique, qui doit vérifier et si nécessaire mettre à jour le document au moins une fois par an.

Pour évaluer l'efficacité et l'adéquation de ce document, les critères suivants doivent être considérés :

- le nombre de changements non effectués en accord avec ce document
- le nombre de changements qui n'ont pas réussi à produire les résultats escomptés

- Fin du document -