GROUPE
PASTEUR
MUTUALITÉ

PSSI GROUPE PASTEUR MUTUALITE

Politique de Sécurité
du Système d'Information

Direction générale	Paloma Gouin
28/02/2022	Responsable Sécurité du Système d'Information

Historique des versions

Version	Date	Rédacteur	Modification
1.0	31/12/2014	Henrik Joulin	Création du document
2.0	16/07/2018	Paloma Gouin	Mise à jour de la structure documentaire basée sur la norme ISO 27002
3.0	17/09/2019	Paloma Gouin	Mise à jour du contenu (enjeux, membres de l'Office, procédure d'alerte, confidentialité des échanges par courriel, PCA, plan de contrôle et indicateurs)
4.0	28/02/2022	Paloma Gouin	Mise à jour du contenu (champ d'application, exigences de sécurité, modalités de l'Office et sécurité liée au RH)

Signataires

Instance	Mode de validation	Date de la validation
Office Sécurité du Système d'Information	Validation formelle et collégiale, cf. compte-rendu de l'Office Sécurité du SI #12	Le 28/02/2022, date de l'Office Sécurité du SI

Sommaire

1. Présentation

La présente politique constitue un cadre de référence qui définit les principes directeurs en matière de protection du système d'information et précise les dispositions à respecter par les entités de Groupe Pasteur Mutualité.

1.1. Objet de la politique de sécurité

L'objet de la politique de sécurité du système d'information est de définir les mesures de sécurité du système d'information permettant d'accompagner la stratégie d'entreprise.

Le cadre réglementaire imposant, la dématérialisation croissante des opérations et des échanges nécessitent une agilité et efficience constante pour le Groupe. Pour répondre à ces enjeux et pour préserver le patrimoine informationnel de l'entreprise de toute menace (connue ou émergente pouvant exposer le système d'information), l'organisation se dote d'une Politique de Sécurité du Système d'Information (**PSSI**).

1.2. Référentiel documentaire

Groupe Pasteur Mutualité dispose d'un référentiel documentaire, constitué d'une charte d'utilisation des technologies de l'information et de communication, de guides et de procédures.

1.3. Champ d'application

La **PSSI** s'applique à l'ensemble du système d'information du **GIE GPM** et de toute société listée dans le champ d'application en annexe. Cette politique concerne l'ensemble des personnes physiques ou morales y intervenant collaborateurs (permanent ou temporaire), conseillers, administrateurs, prestataires et leurs sous-traitants.

Ci-après, toute information mentionnant Groupe Pasteur Mutualité ou le Groupe fera référence au champ d'application tel que précité.

2. Contexte

Les enjeux présentés ci-dessous relèvent de la volonté de Groupe Pasteur Mutualité de maîtriser et de gérer les risques associés au système d'information, de préserver et d'accroître sa performance, de renforcer la confiance auprès de ses adhérents, partenaires et d'assurer une conformité légale et règlementaire.

2.1. Enjeux de la stratégie sécurité du système d'information

Le **respect de la conformité réglementaire** doit permettre au Groupe de répondre de manière appropriée à l'application du cadre réglementaire, d'apporter des éléments pertinents et de donner de la visibilité aux membres de l'Office Sécurité du Système d'Information, aux instances du Groupe, aux auditeurs sur la gestion des risques en lien à la cybersécurité.

La **résilience et protection du patrimoine informationnel** doit contribuer à une sécurisation pertinente des informations et répondre favorablement aux enjeux d'un écosystème élargi (mobilité et nouveaux usages, sites distants, réseau commercial de proximité, ...).

La **sécurité digitale et innovation** vise à mettre à disposition des métiers des solutions pragmatiques de sécurisation, d'offrir des solutions adaptées aux nouveaux usages et de sécuriser sans restreindre l'initiative des métiers.

Enfin, la **gouvernance sécurité de l'information** a pour objet de donner une lisibilité claire sur les rôles en matière de protection du patrimoine informationnel, de disposer d'une agilité et d'une efficacité constante dans les prises de décisions.

2.2. Exigences de sécurité

Les exigences listées ci-dessous, font état des objectifs métiers qui sont attendus :

- un besoin de disponibilité des données pour la réalisation des activités métier et la production des états réglementaires, ainsi que pour les services offerts aux tiers,
- un besoin d'intégrité des données et des traitements, pour l'exactitude des opérations (valeurs liquidatives, dates d'échéances…), pour le pilotage et le contrôle des activités (gestion de trésorerie, comptabilité, statistiques, qualité des données, archivage réglementaire…),
- un besoin de confidentialité pour le traitement de données et pour toute autre information soumise à une obligation légale ou réglementaire de confidentialité,
- un besoin de disposer des éléments de preuve dans les applications métier (pistes d'audit, imputabilité des opérations à leurs auteurs…) pour l'investigation a posteriori et pour faciliter les activités de contrôle interne et d'audit.

3. Structure documentaire

La politique de sécurité du système d'information est déclinée en quatorze catégories basées sur la norme internationale relative la sécurité de l'information (**ISO 27002**).

Nomenclature des catégories

Identification	Catégories ISO 27002
PSI	Politique de sécurité de l'information
ORG	Organisation de la Sécurité de l'Information
PER	Sécurité des ressources humaines
ACT	Gestion des actifs
CTR	Contrôle d'accès
CRY	Cryptographie
PHY	Sécurité physique et environnementale
EXP	Sécurité liée à l'exploitation
COM	Sécurité des communications
ACQ	Acquisition, développement et maintenance des systèmes d'information
REL	Relations avec les fournisseurs
INC	Gestion des incidents liés à la sécurité de l'information
GCA	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
CON	Conformité

Les catégories précitées font l'objet de règles spécifiques. Ces dernières suivent la nomenclature suivante « **R-XXX-Y.Y** », où **XXX** et **Y.Y** font respectivement référence à une catégorie et à la numérotation associée.

4. Terminologie

GIE GPM : Groupement d'intérêt économique rattaché au Groupe Pasteur Mutualité

Système d'information : Le système d'information (SI) est défini comme l'ensemble des dispositifs matériels, logiciels, et organisationnels, qui interagissent de façon à conserver, traiter et communiquer des informations

Sécurité du système d'information : La sécurité du système d'information est définie comme l'ensemble des moyens, mesures, dispositions et structures organisationnelles qui protègent le système d'information dans sa totalité ainsi que tous les acteurs associés

Disponibilité : Aptitude du SI à garantir l'exécution des traitements et l'accès aux informations dans des conditions prédéfinies

Intégrité : Aptitude du SI à assurer que les informations sont inaltérables dans le temps et dans l'espace

Confidentialité : Aptitude du SI à protéger les informations sensibles de toute divulgation non autorisée

Preuve : Aptitude du SI à fournir des pistes d'audit et les éléments de preuve correspondant aux actions réalisées

PCA : Politique Continuité d'Activité qui définit les règles et responsabilités de Groupe Pasteur Mutualité et de chacun de ses collaborateurs afin de permettre à assurer les prestations de services et autres tâches opérationnelles essentielles ou importantes de l'entreprise puis la reprise des activités

Norme ISO 27002 : Norme internationale relative à la sécurité de l'information

RGPD : Règlement général sur la protection des données mis en vigueur le 25 mai 2018

HaDS : Hébergeur agréé de données de santé

OSSI : Office Sécurité du Système d'Information

RSSI : Responsable Sécurité du Système d'Information

Risque cyber : Les risques cyber se déclinent en conséquence diverses, affectant directement ou indirectement la sécurité des informations de l'entreprise (cybercriminalité, atteinte à l'image, espionnage, sabotage)

CNIL : Commission nationale de l'informatique et des libertés

Solvabilité II : Ensemble de règles fixant le régime de solvabilité applicables aux entreprises d'assurances dans l'Union Européenne, entré en application le 1er janvier 2016

ACPR : Autorité de contrôle prudentiel et de résolution, chargée de la supervision des secteurs bancaires et d'assurance

CESIN : Club des Experts de la Sécurité de l'Information et du Numérique

5. Principes de la politique de sécurité

5.1. Orientations de la direction en matière de sécurité de l'information

5.1.1. Politiques de sécurité de l'information

R-PSI-1.1 : Groupe Pasteur Mutualité dispose d'une politique de sécurité du système d'information qui fait l'objet d'une publication en interne.

R-PSI-1.2 : La politique de sécurité du système d'information est validée et approuvée, de manière collégiale, par les membres de l'Office de Sécurité du Système d'Information.

R-PSI-1.3 : L'Office Sécurité du Système d'Information (**OSSI**) est l'instance stratégique dédiée à la sécurité du SI au sein de Groupe Pasteur Mutualité, et en charge du pilotage d'une crise majeure en matière de cybersécurité. Cette instance trimestrielle, dont la composition figure en annexe, donne lieu à un compte-rendu.

R-PSI-1.4 : La validation de la présente et des versions supérieures s'inscrit à l'ordre du jour de l'Office Sécurité du Système d'Information.

R-PSI-1.5 : Groupe Pasteur Mutualité dispose d'indicateurs permettant d'assurer le suivi de l'activité liée à la sécurité du système d'information.

5.1.2. Revues des politiques de sécurité de l'information

R-PSI-1.6 : La politique de sécurité du SI est revue périodiquement mais également en cas de changement majeur (évolution contextuelle, technologique ou règlementaire).

6. Organisation de la sécurité de l'information

L'organisation de la sécurité de l'information du **GIE GPM** est sous la responsabilité de l'administrateur unique. Le Responsable Sécurité du Système d'Information (RSSI) est rattaché auprès du dirigeant opérationnel d'**AGMF Prévoyance** et dispose d'un droit d'accès direct.

6.1. Organisation interne

6.1.1. Fonctions et responsabilités liées à la sécurité de l'information

R-ORG-1.1 : Les responsabilités en matière de sécurité du SI sont définies et attribuées au Responsable Sécurité du Système d'information.

R-ORG-1.2 : Le prestataire en charge de l'infogérance s'engage par ailleurs à respecter les engagements pris et contractualisés dans le cadre de l'externalisation du SI de GPM.

6.1.2. Séparations des tâches

R- ORG-1.3 : Une séparation des tâches est appliquée selon les activités et les directions.

6.1.3. Relations avec les autorités

R-ORG-1.4 : L'organisation peut être amenée à entretenir des contacts ou des relations appropriées avec les autorités compétentes, si nécessaire.

6.1.4. Relations avec des groupes de travail spécialisés

R-ORG-1.5 : Le RSSI entretient des contacts ou des relations appropriées avec des groupes de spécialistes et les autorités compétentes.

6.1.5. Sécurité de l'information dans la gestion de projet

R-ORG-1.6 : La sécurité de l'information est prise en compte dans les projets avec une intégration de la sécurité du SI dès l'évaluation d'un projet.

6.2. Appareils mobiles et télétravail

6.2.1. Politique en matière d'appareils mobiles

R-ORG-2.1 : Des mesures de sécurité sont appliquées pour l'utilisation d'appareils mobiles fournis par le service Informatique Transverse.

6.2.2. Télétravail

R-ORG-2.2 : Des mesures de sécurité sont appliquées et définies dans la charte d'utilisation des technologies de l'information et de communication, dans le cadre des nouvelles modalités de connexion.

7. Sécurité liée aux ressources humaines

7.1. Avant l'embauche

7.1.1. Sélection des candidats

R-PER-1.1 : Une vérification des informations concernant les candidats à l'embauche est réalisée.

R-PER-1.2 : Toutefois, qu'il s'agisse de postulants, de contractants ou d'utilisateurs tiers, les vérifications des informations concernant tous les candidats doivent être réalisées conformément aux lois, aux règlements et à l'éthique et doivent être proportionnelles aux exigences métier, à la sensibilité des informations accessibles et aux risques identifiés.

R-PER-1.3 : La charte d'utilisation des technologies de l'information et de communication est communiquée au collaborateur qui s'engage à la respecter.

7.1.2. Sensibilisation, apprentissage et formation à la sécurité de l'information

R-PER-1.4. : Des engagements contractuels sont conclus avec les prestataires de Groupe Pasteur Mutualité intervenant au sein de la direction des Ressources Humaines.

7.2. Pendant la durée du contrat

7.2.1. Responsabilités de la direction

R-PER-2.1 : Les directions concernées sont garantes du respect des règles de sécurité auprès de ses collaborateurs et de ses contractants.

R-PER-2.2 : La charte d'utilisation des technologies de l'information et de communication est annexée au règlement intérieur et fait l'objet d'une publication en interne sur l'intranet.

7.2.2. Sensibilisation, apprentissage et formation à la sécurité de l'information

R-PER-2.3 : Des actions de sensibilisation et de communication à destination des collaborateurs sont réalisées au sein du Groupe.

R-PER-2.4 : Des rappels aux règles et bonnes pratiques sur le thème de la sécurité du SI sont réalisés, ainsi que des mises en situation et des tests aléatoires.

7.2.3. Processus disciplinaire

R-PER-2.5 : Le non-respect des règles liées à la sécurité de l'information et de la charte d'utilisation des technologies de l'information et de communication, peut constituer une cause d'engagement de mesures disciplinaires pouvant aller jusqu'au licenciement au regard du règlement intérieur et du code du travail.

7.3. Rupture, terme ou modification du contrat de travail

7.3.1. Achèvement ou modification des responsabilités associées au contrat de travail

R-PER-3.1 : En cas de départ ou de mutation, les ressources humaines informent le service Informatique Transverse du mouvement d'un collaborateur.

R-PER-3.2 : L'ensemble des managers et des Directions concernées, veille à l'application des responsabilités par les collaborateurs et les contractants.

R-PER-3.3 : Une attention particulière est portée à la clause de non-concurrence, à la restitution des actifs et au retrait des droits d'accès, lors d'un départ d'un collaborateur ou d'un prestataire.

8. Gestion des actifs

8.1. Responsabilités relatives aux actifs

8.1.1. Inventaire des actifs

R-ACT-1.1 : Les actifs associés à l'information et aux moyens de traitement de l'information sont identifiés.

R-ACT-1.2 : L'inventaire des actifs (matériel et applicatif) est mis à jour périodiquement.

R-ACT-1.3 : La gestion du parc matériel fait l'objet d'une procédure du contrôle interne.

8.1.2. Propriété des actifs

R-ACT-1.5 : Des responsables d'application sont identifiés et une base de connaissance est mise à disposition.

R-ACT-1.6 : Les utilisateurs sont responsables de l'utilisation de toute ressource de traitement de l'information sous leur responsabilité et/ou de toute utilisation effectuée avec leurs identifiants.

8.1.3. Utilisation correcte des actifs

R-ACT-1.7 : Des règles de sécurité permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information sont définies, mises en œuvre et révisées périodiquement par le propriétaire (ou son délégataire) des actifs concernés. Celles-ci sont précisées dans la charte d'utilisation des technologies de l'information et de communication.

8.1.4. Restitution des actifs

R-ACT-1.8 : La totalité des actifs est restituée par les collaborateurs au terme de leur période d'emploi, contrat ou accord.

8.2. Manipulation des supports

8.2.1. Mise en rebut

R-ACT-2.1 : Les supports qui ne servent plus sont mis au rebut de manière sécurisée et suivent le processus établi.

9. Contrôle d'accès

9.1. Exigences métier en matière de contrôle d'accès

9.1.1. Politique de contrôle d'accès

R-CTR-1.1 : Le contrôle d'accès mis en place permet d'appliquer les droits appropriés aux fonctions spécifiques de l'utilisateur et d'autoriser l'accès le cas échéant.

R-CTR-1.2 : Les habilitations s'appuient sur les informations provenant des ressources humaines et des directions concernées, pour la création des accès.

R-CTR-1.3 : Une politique de gestion des mots de passe est appliquée par l'ensemble des utilisateurs.

9.1.2. Accès aux réseaux et aux services en réseau

R-CTR-1.4 : L'accès au système d'information prévoit des mesures techniques et des processus de gestion des paramètres permettant de protéger les ressources informatiques contre des accès illicites.

9.2. Gestion de l'accès utilisateur

9.2.1. Enregistrement et désinscription des utilisateurs

R-CTR-2.1 : Une procédure pour l'attribution et le retrait des droits d'accès est définie :

- les utilisateurs (interne, externe, permanent ou temporaire) disposent d'identifiants uniques,
- des mécanismes d'authentification et d'habilitation sont mis en œuvre.

R-CTR-2.2 : La durée des habilitations accordée au personnel temporaire (CDD, prestataire, intérimaire, stagiaire…) correspond à la durée spécifiée dans leur contrat, par défaut cette durée est limitée.

9.2.2. Maîtrise de la gestion des accès utilisateur

R-CTR-2.3 : Toute création de compte utilisateur est réalisée dans le respect des principes de moindre privilège correspondant strictement au périmètre du collaborateur. Une demande de la part des ressources humaines et/ou des directions concernées est nécessaire pour l'obtention d'habilitations complémentaires.

9.2.3. Gestion des privilèges d'accès

R-CTR-2.4 : L'attribution et l'utilisation des comptes à privilèges sont contrôlées et restreintes. La gestion des comptes à hauts privilèges fait l'objet d'une procédure de contrôle interne.

9.2.4. Revue des droits d'accès utilisateur

R-CTR-2.5 : Une revue des droits d'accès utilisateur au travers de contrôles périodiques est réalisée.

9.2.5. Suppression ou adaptation des droits d'accès

R-CTR-2.6 : Les droits d'accès de tous les salariés et tiers sont supprimés en cas de modification ou à la fin de leur contrat.

9.3. Contrôle de l'accès au système et aux applications

9.3.1. Restriction d'accès à l'information

R-CTR-3.1 : L'accès aux systèmes et aux applications est contrôlé et tracé.

R-CTR-3.2 : L'utilisation des programmes permettant de contourner les mesures de sécurité est contrôlée.

9.3.2. Sécuriser les procédures de connexion

R-CTR-3.3 : Le personnel informatique assurant l'exploitation des équipements et le développement des outils informatiques, dispose d'habilitations octroyées selon des règles définies dans le respect des principes déontologiques et compatibles avec les objectifs de production et de bon fonctionnement de l'entreprise.

R-CTR-3.4 : L'accès au système d'information au travers des dispositifs en mobilité (nouvelles modalités de connexion des utilisateurs et connexions distantes par des sous-traitants) respecte les normes techniques et les règles permettant de maintenir un niveau de sécurité adapté.

9.3.3. Contrôle d'accès au code sources des programmes

R-CTR-3.5 : L'accessibilité au code source des applications est restreint.

10. Cryptographie

10.1. Mesures cryptographiques

10.1.1. Politique d'utilisation des mesures cryptographiques

R-CRY-1.1 : Des mesures cryptographiques sont définies pour le chiffrement des postes de travail, pour l'authentification au réseau filaire et sans-fil.

R-CRY-1.2 : Des mesures cryptographiques sont définies pour l'utilisation de signature électronique et les connexions en mobilité.

R-CRY-1.3 : Des certificats de confiance sont publiés sur les sites gérés par Groupe Pasteur Mutualité.

10.1.2. Gestion des clés

R-CRY-1.4 : Les algorithmes de chiffrement, la longueur des clés et les pratiques d'utilisation respectent les bonnes pratiques en la matière.

11. Sécurité physique et environnementale

11.1. Zones sécurisées

11.1.1. Périmètre de sécurité physique

R-PHY-1.1 : Des périmètres de sécurité servant à protéger les zones sensibles, critiques existent.

R-PHY-1.2 : Des mesures proportionnelles et adaptées au niveau de sensibilité des actifs concernés sont mises en œuvre pour empêcher l'accès non autorisé aux locaux de l'entreprise.

11.1.2. Contrôles physiques des accès

R-PHY-1.3 : Les zones sécurisées des centres de données hébergeant les actifs de Groupe sont protégées et contrôlées.

11.1.3. Sécurisation des bureaux, des salles et des équipements

R-PHY-1.4 : Des mesures de sécurité physique sont appliquées à l'accès des locaux.

11.1.4. Protection contre les menaces extérieures et environnementales

R-PHY-1.5 : Des mesures de protection physique contre les désastres naturels et les attaques malveillantes sont mises en œuvre. Les infrastructures de traitement des données doivent être situées dans des zones de sécurité protégées de façon à réduire les risques présentés par les menaces et les dangers liés à l'environnement, notamment en matière de dégâts des eaux, d'incendie, de rupture des énergies, et ainsi contribuer à la garantie de continuité des services.

11.1.5. Zones de livraison et de chargement

R-PHY-1.6 : Les zones de livraison et de chargement sont contrôlées dans les centres de données hébergeant les actifs de Groupe Pasteur Mutualité.

11.2. Matériels

11.2.1. Emplacement et protection du matériel

R-PHY-2.1 : L'emplacement du matériel est déterminé et protégé pour réduire les dangers environnementaux et les accès non autorisé.

11.2.2. Services généraux

R-PHY-2.2 : Le matériel est protégé contre les coupures de courants et défaillances des services généraux. Cette protection s'applique à tous les équipements qu'il s'agisse du cœur de réseau, des systèmes de câblage ou des équipements de routage périphériques.

11.2.3. Sécurité du câblage

R-PHY-2.3 : Les câbles électriques et de télécommunication transportant des données ou supportant les services d'information doivent être protégés sur site et dans les centres de données.

11.2.4. Maintenance du matériel

R-PHY-2.4 : La continuité du service doit être assurée par des équipements en parfait état de fonctionnement, qu'il s'agisse des équipements informatiques eux-mêmes ou des équipements logistiques d'infrastructure. Ils doivent donc être couverts par des contrats de maintenance adaptés et testés périodiquement.

11.2.5. Sécurité du matériel et des actifs hors des locaux

R-PHY-2.5 : Les matériels sont la propriété du Groupe. À ce titre, ils ne doivent pas sortir d'un site sans l'autorisation du responsable de la gestion de cet équipement.

11.2.6. Mise au rebut ou recyclage sécurisé(e) du matériel

R-PHY-2.6 : Afin d'assurer la confidentialité des données, des processus sont mis en œuvre pour effacer les données des supports avant toute mise au rebut.

R-PHY-2.7 : Dans le cas d'envoi en maintenance ou en destruction, il convient de s'assurer au préalable de la sensibilité des données et des moyens de protection mis en œuvre.

12. Sécurité liée à l'exploitation

12.1. Procédures et responsabilités liées à l'exploitation

12.1.1. Procédures d'exploitation documentées

R-EXP-1.1 : Les procédures d'exploitation sont documentées et mises à disposition de tous les utilisateurs concernés.

12.1.2. Gestion des changements

R-EXP-1.2 : Les changements apportés à l'organisation et aux moyens de traitement de l'information sont contrôlés dans le cadre des évolutions et des mises en production.

12.1.3. Dimensionnement

R-EXP-1.3 : Des projections sur les dimensionnements futurs sont réalisés pour garantir les performances nécessaires du système afin de garantir la disponibilité d'une puissance de traitement et d'un stockage adéquat.

12.1.4. Séparation des environnements de développement, de test et d'exploitation

R-EXP-1.4 : Les environnements de développement sont séparés de ceux de test et de production afin d'éviter de corrompre tout environnement.

12.2. Protection contre les logiciels malveillants

12.2.1. Mesures contre les logiciels malveillants

R-EXP-2.1 : Des mesures sont appliquées pour se protéger contre les logiciels malveillants.

R-EXP-2.2 : Des messages de communication sont réalisés pour sensibiliser les collaborateurs sur cette thématique.

12.3. Sauvegarde

12.3.1. Sauvegarde des informations

R-EXP-3.1 : Des copies de sauvegardes sont réalisées selon une fréquence et une rétention définie, conformément aux exigences établies dans le contrat d'infogérance.

R-EXP-3.2 : Les supports de sauvegarde sont externalisés en respectant des conditions de sécurité importantes.

R-EXP-3.3 : Les données des serveurs applicatifs et des serveurs techniques qui concourent au fonctionnement de l'activité du Groupe doivent faire l'objet de sauvegardes complètes et cohérentes.

R-EXP-3.4 : Les exigences en matière de conservation et de protection des copies de sauvegarde sont définies.

12.4. Journalisation et surveillance

12.4.1. Journalisation des évènements

R-EXP-4.1 : Une journalisation des événements est réalisée permettant d'assurer une corrélation.

12.4.2. Protection de l'information journalisée

R-EXP-4.2 : Des moyens de protection des journaux d'évènements sont définis.

12.4.3. Journaux administrateur et opérateur

R-EXP-4.3 : Les activités des administrateurs sont tracées et les informations sont exploitables.

12.4.4. Synchronisation des horloges

R-EXP-4.4 : Les horloges des systèmes sont synchronisées sur une source de référence temporelle unique.

12.5. Maîtrise des logiciels en exploitation

12.5.1. Installation de logiciels sur des systèmes en exploitation

R-EXP-5.1 : L'installation de logiciels sur les systèmes en exploitation est contrôlée.

12.6. Gestion des vulnérabilités techniques

12.6.1. Gestion des vulnérabilités techniques

R-EXP-6.1 : Les vulnérabilités techniques des systèmes d'information en exploitation sont remontées aux équipes opérationnelles et suivent le processus de gestion des changements.

12.6.2. Restrictions liées à l'installation de logiciels

R-EXP-6.2 : Les utilisateurs ne sont pas en capacité d'installer un logiciel sur le poste de travail. Toute installation est encadrée par un collaborateur du service Informatique.

13. Sécurité des communications

13.1. Management de la sécurité des réseaux

13.1.1. Contrôle des réseaux

R-COM-1.1 : Les réseaux sont gérés et contrôlés afin de protéger l'information dans les systèmes et les applications.

R-COM-1.2 : Les réseaux du Groupe font l'objet d'une protection permettant la transmission dans des conditions d'intégrité, de disponibilité et de confidentialité.

R-COM-1.3 : Des mesures de protection et de surveillance sont appliquées pour les services en ligne. Une attention particulière est apportée à l'intégrité et à la confidentialité des données.

R-COM-1.4 : Tout accès d'un utilisateur, par un réseau sans fil, à une zone de confiance non publique, doit garantir la confidentialité des échanges.

R-COM-1.5 : Tout point d'accès, interne, sans fil à Internet, doit assurer l'authentification de l'accédant.

13.1.2. Cloisonnement des réseaux

R-COM-1.6 : Un cloisonnement des réseaux est appliqué.

13.2. Transfert de l'information

13.2.1. Politiques et procédures de transfert de l'information

R-COM-2.1 : Des mesures sont mises en œuvre pour protéger les transferts d'information transitant par tout type d'équipement de communication.

13.2.2. Accords en matière de transfert d'information

R-COM-2.2 : Les exigences en matière d'engagement de confidentialité et de non-divulgation sont appliquées.

14. Acquisition, développement et maintenance des systèmes d'information

14.1. Exigences de sécurité applicables aux systèmes d'information

14.1.1. Analyse et spécification des exigences de sécurité de l'information

R-ACQ-1.1 : Groupe Pasteur Mutualité intègre une démarche de prise en compte de la sécurité dans les projets et veille à ce que les développements réalisés pour son compte comportent cette dimension.

R-ACQ-1.2 : Les exigences liées à la sécurité de l'information sont reprises dans les nouveaux systèmes d'information.

R-ACQ-1.3 : Ces exigences sont prises en compte lorsque des changements sont apportés aux systèmes existants.

14.2. Sécurité des processus de développement et d'assistance technique

14.2.1. Politique de développement sécurisé

R-ACQ-2.1 : Les règles de développement des logiciels et des systèmes existent et sont appliquées aux développements de l'organisation.

14.2.2. Environnement de développement sécurisé

R-ACQ-2.2 : Un environnement est dédié aux tâches de développement et d'intégration du système. Ces environnements font l'objet d'un cloisonnement et les codes sources sont protégés.

15. Relations avec les fournisseurs

15.1. Sécurité de l'information dans les relations avec les fournisseurs

15.1.1. Politique de sécurité de l'information dans les relations avec les fournisseurs

R-REL-1.1 : Les exigences de sécurité de l'information pour limiter les risques d'accès aux actifs de l'organisation par le fournisseur sont définies contractuellement.

R-REL-1.2 : Les exigences liées à la sécurité de l'information sont établies et convenues avec le fournisseur.

15.1.2. La sécurité dans les accords conclus avec les fournisseurs

R-REL-1.3 : Les accords conclus avec les fournisseurs incluent des exigences sur le traitement des risques de sécurité de l'information.

R-REL-1.4 : Les mesures existantes sont gérées en tenant compte de la criticité de la sous-traitance.

15.2. Gestion de la prestation de service

15.2.1. Surveillance et revue des services des fournisseurs

R-REL-2.1 : Les directions concernées surveillent périodiquement la prestation des fournisseurs intervenant sur le système d'information.

16. Gestion des incidents liés à la sécurité de l'information

16.1. Gestion des incidents liés à la sécurité de l'information et améliorations

16.1.1. Responsabilités et procédures

R-INC-1.1 : Les incidents de sécurité sont formalisés.

R-INC-1.2 : Un centre opérationnel de sécurité assure la détection des menaces afin de répondre efficacement en cas d'incident majeur.

R-INC-1.3 : En cas d'incident de sécurité avéré, le **RSSI**, alerte l'**OSSI** et organise la réponse selon le périmètre et le niveau de sévérité de l'incident.

16.1.2. Signalement des événements liés à la sécurité de l'information

R-INC-1.4 : Les événements liés à la sécurité de l'information sont signalés dans les meilleurs délais par les parties prenantes.

R-INC-1.5 : Un dispositif d'alerte des incidents de sécurité est défini et publié sur l'intranet.

16.1.3. Signalement des failles liées à la sécurité de l'information

R-INC-1.6 : Dans le cadre de l'infogérance, les équipes du service Informatique sont alertées dans les meilleurs délais dès la connaissance d'une faille liée à la sécurité de l'information. En complément, une veille est réalisée par le RSSI auprès des services compétents (ANSSI, CESIN, ou autre).

16.1.4. Réponse aux incidents liés à la sécurité de l'information

R-INC-1.7 : Des dispositifs pour répondre aux besoins de prévention, détection, réaction, traitement et suivi des événements et des incidents relatifs à la Sécurité du SI sont mis en œuvre.

16.1.5. Appréciation des événements liés à la sécurité de l'information et prise de décision

R-INC-1.8 : Les événements liés à la sécurité de l'information sont appréciés et classés comme incidents liés à la sécurité si nécessaire.

16.1.6. Tirer des enseignements des incidents liés à la sécurité de l'information

R-INC-1.9 : Les incidents sont analysés et les informations liées à la résolution des incidents sont formalisés. Ceci afin de réduire la probabilité ou les conséquences d'incidents ultérieurs.

16.1.7. Recueil de preuves

R-INC-1.10 : Selon la catégorisation et l'impact de l'incident de sécurité, un recueil de preuves peut être réalisé.

17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

17.1. Continuité de la sécurité de l'information

17.1.1. Organisation de la continuité de la sécurité de l'information

R-GCA-1.1 : La sécurité de l'information est prise en compte dans la gestion de la continuité de l'activité. L'organisation mise en place dans le cadre de la gestion de la continuité de l'activité permet de déterminer les actions nécessaires à la résolution d'un incident majeur et d'activer le cas-échéant la cellule de crise.

R-GCA-1.2 : Dans le cadre de la gestion de la continuité de l'activité, une analyse de sinistralité est identifiée afin de permettre aux entités de Groupe Pasteur Mutualité de définir et de prioriser les scénarios de risques.

R-GCA-1.3 : Groupe Pasteur Mutualité dispose d'une politique de Continuité d'activité.

17.2. Redondances

17.2.1. Disponibilité des moyens de traitement de l'information

R-GCA-2.1 : Des moyens de traitement de l'information sont mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.

R-GCA-2.2 : Le plan de secours informatique qui fait l'objet d'une planification périodique permet de s'assurer de la disponibilité d'un composant du SI.

18. Conformité

18.1. Conformité aux obligations légales et réglementaires

18.1.1. Identification de la législation et des exigences contractuelles applicables

R-CON-1.1 : Les exigences réglementaires et contractuelles sont définies et documentées. Les activités de sous-traitance critique impactant le SI du **GIE GPM** font l'objet d'une attention particulière.

R-CON-1.2 : La PSSI doit permettre d'assurer le respect des obligations légales et réglementaires qui lui sont imposées (**RGPD**, **CNIL**, **Solvabilité II**, **ACPR**, ...).

R-CON-1.3 : Le dispositif de maîtrise des risques de cybersécurité est défini et exécuté afin d'assurer le respect des règles de sécurité de l'information au sein du Groupe.

R-CON-1.4 : Des mesures visant à assurer le maintien de la confidentialité des informations qui sont amenés à être échanger par mail en interne ou avec des tiers sont appliquées.

18.1.2. Protection de la vie privée et protection des données à caractère personnel

R-CON-1.5 : Des mesures de sécurité sont définies dans les registres de traitements.

R-CON-1.6 : Des mesures de sécurité sont appliquées pour se mettre en conformité à l'hébergement agréé de données de santé.

18.2. Revue indépendante de la sécurité de l'information

18.2.1. Revue indépendante de la sécurité de l'information

R-CON-2.1 : Des revues régulières et indépendantes de la méthode de gestion et de la mise en œuvre de la sécurité de l'organisation sont réalisées périodiquement.

R-CON-2.2 : Le plan pluriannuel de l'audit interne précise le périmètre et le calendrier des missions liées au système d'information.

18.2.2. Examen de la conformité technique

R-CON-2.3 : Des audits de vulnérabilité, ou tests d'intrusion, qui font partie du dispositif de contrôle permanent, sont menés périodiquement, afin de vérifier la conformité technique du système d'information aux exigences de sécurité de la présente PSSI.

R-CON-2.4 : Le référentiel d'authentification fait l'objet d'une évaluation périodique.