Politique Générale de Sécurité des Systèmes d'Information

(PGSSI)

Réf : PO_SI_01

	Nom	Entité	Date
Rédacteur(s)	Abdellah BAGDAD / RSSI	Département Sécurité SI	14/06/2021
Vérificateur(s)	- Amine Trabelsi/DSI - Evelyne Munoz/DPO - Driss BENHAMIDA/Chief Compliance & Risk Officer - Yazid EL ALAOUI YAZIDI/Directeur Qualité	Direction SI Direction Qualité	24/06/2021
Approbateur(s)	Youssef EL AOUFIR/Directeur Général	Direction Générale	30/06/2021

Historique des versions :

Date	Référence du document	Version	Objet de la mise à jour	Auteur
02/01/2019	PO-SI-01	1.0	Création du document	Département Sécurité SI
14/06/2021	PO-SI-01	2.0	Revue générale du document	Département Sécurité SI

SOMMAIRE

I. ENJEUX DE LA SECURITE DES SYSTEMES D'INFORMATION 4

II. OBJECTIFS ET PRINCIPES DE MISE EN ŒUVRE DE LA POLITIQUE 4

III. DOMAINE D'APPLICATION 6

IV. OBLIGATION LEGALES ET REGLEMENTAIRES 6

V. DIFFUSION 6

VI. ROLES ET RESPONSABILITES DANS LE CADRE DE LA MISE EN ŒUVRE DE LA PGSSI 6

VI.1 LA DIRECTION GENERALE 6

VI.2 LE RESPONSABLE DE LA SECURITE DES SYSTEMES D'INFORMATION (RSSI) 7

VI.3 LE DIRECTEUR DES SYSTEMES D'INFORMATION 8

VI.4 LES RESPONSABLES D'ENTITES SI 8

VI.5 LES CHEFS DE PROJET SI 8

VI.6 LES ADMINISTRATEURS SI 8

VI.7 LES LIGNES METIERS ET LES DIRECTIONS CENTRALES 8

VII. INSTANCES DE PILOTAGE 10

VII.1 Comité Directeur de Sécurité 10

VII.1.1 Objectifs du CDS 10

VII.1.2 Pilotage 10

VII.1.3 Missions du CDS 10

VII.1.4 Membres du CDS 10

VII.1.5 Fréquences de réunions et livrables 11

VII.2 Comité Opérationnel de sécurité 11

VII.2.1 Objectif du COS 11

VII.2.2 Missions du COS 11

VII.2.3 Membres du COS 11

VII.2.4 Fréquence des réunions et livrables 11

VIII. CORPUS DOCUMENTAIRE DE SECURITE DES SYSTEMES D'INFORMATION 11

I. ENJEUX DE LA SECURITE DES SYSTEMES D'INFORMATION

Les Systèmes d'Information (ou SI) gèrent notamment des données contractuelles, métiers, financières ainsi que des données nominatives de clients et du personnel Intelcia.

L'ensemble de ces données constitue un patrimoine stratégique d'informations, exposé à des risques de sécurité et soumis à des obligations légales et réglementaires, et devant être protégé efficacement.

Les enjeux de la Sécurité des Systèmes d'Information (ou SSI) sont primordiaux pour Intelcia et s'inscrivent dans la volonté du Groupe :

- d'être en conformité avec les lois et règlements nationaux et internationaux ;
- de renforcer la confiance des clients et des partenaires ;
- de s'ouvrir davantage aux clients et partenaires, et de produire de nouveaux services en faisant de la sécurité un facteur d'opportunité et de croissance ;
- de contribuer à la performance globale du Groupe en réduisant le nombre d'incidents ainsi que leurs impacts et en optimisant l'allocation des ressources dédiées à la sécurité ;
- d'anticiper et de gérer au mieux toute situation de risque sur les Systèmes d'Information, en particulier relatif à la cybercriminalité.

II. OBJECTIFS ET PRINCIPES DE MISE EN ŒUVRE DE LA POLITIQUE

L'information et les processus, systèmes et réseaux qui en permettent le traitement constituent des actifs importants pour Intelcia dans la réalisation de sa mission. La politique de sécurité de l'information a pour objectif d'assurer un niveau adéquat de sécurité en termes de confidentialité, disponibilité et d'intégrité des actifs informationnels de Intelcia contre toutes les menaces dont elle pourrait être l'objet.

La Sécurité des Systèmes d'Information (ou SSI) d'Intelcia a pour objectifs de :

- Assurer la couverture des menaces et risques identifiés en matière de cybercriminalité ou de manquements internes (attaques SI, fraudes internes ou externes, fuites d'informations, indisponibilités des systèmes) ;
- Mettre en place la gouvernance de gestion des risques SSI (homogénéiser la méthodologie de gestion des risques, protéger en priorité les applications et ressources les plus sensibles du Groupe, contribuer à la définition et à la mise en œuvre des contrôles du domaine de la SSI) ;
- Accompagner la transformation du Groupe et du modèle opérationnel en matière de Sécurité des Systèmes d'Information.

Ces orientations sont déclinées par les lignes-métiers et les directions centrales, selon une approche graduelle et mesurée, respectant les principes suivants :

1) **conformité aux lois et aux règlementations**;

2) priorisation des actions à partir de l'**identification et l'évaluation des risques Métier en lien avec le Système d'Information,** et la prise en compte effective de la Sécurité des Systèmes d'Information dans chaque projet ;

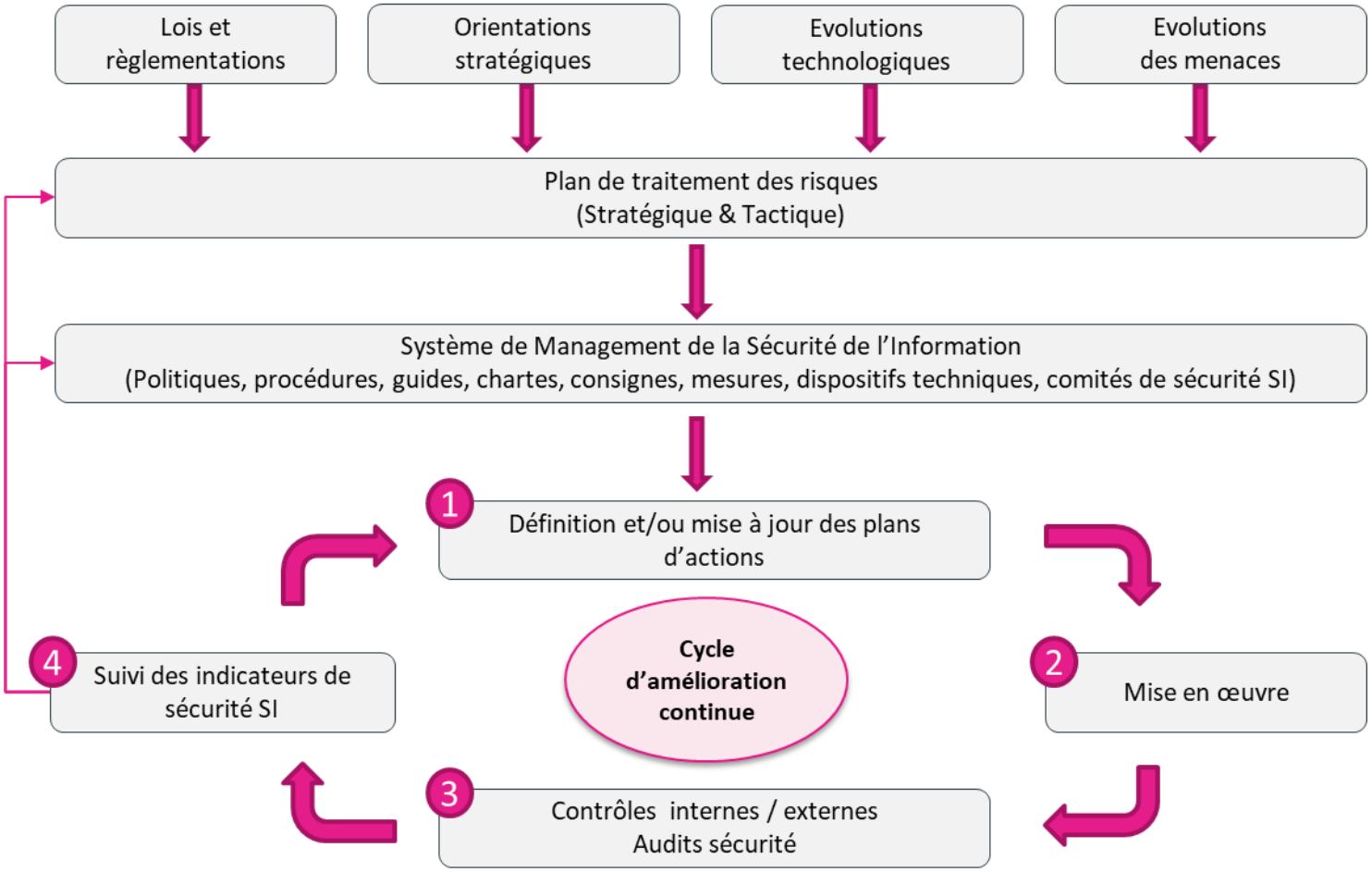
3) mise en place et pilotage du **Système de Management de la Sécurité de l'Information** (ou SMSI) adéquat et documenté qui repose sur une organisation claire, des processus documentés, un suivi des incidents, des dispositifs de veille, de détection et de réaction, des processus de contrôle, un dispositif de reporting permettant de mesurer l'aptitude du Groupe à se protéger et les progrès accomplis dans le temps ;

4) **accroissement de la vigilance** notamment via des actions de **sensibilisation et de formation** ;

5) **renforcement des engagements contractuels** (clauses sécurité) et des **contrôles des prestataires et partenaires** ;

6) **respect des fondements** permettant d'assurer **la maîtrise des accès aux SI** par les personnels, les partenaires et les clients, ainsi que **la protection des informations sensibles**.

Ces principes peuvent se traduire selon la vue d'ensemble suivante :



Vue d'ensemble de la sécurité

III. DOMAINE D'APPLICATION

La présente politique s'applique à l'ensemble du patrimoine informationnel d'Intelcia, tout au long de son cycle de vie et quels que soient les supports, les vecteurs de transmission, et leur localisation.

Tout utilisateur (salarié, stagiaire, consultant, prestataire de services, intérimaire ou tout autre utilisateur ayant accès au système d'information) doit participer activement, en fonction de son niveau de responsabilité et des tâches qu'il exerce, à la mise en œuvre et au respect de la politique Générale de Sécurité des Systèmes d'Information.

IV. OBLIGATION LEGALES ET REGLEMENTAIRES

En tant qu'acteur majeur dans le domaine de la relation client présent aussi bien au Maroc qu'à l'international, le Groupe Intelcia doit être en conformité avec les obligations réglementaires de chaque pays en matière de sécurité des systèmes d'information et de protection des données personnelles, notamment les suivantes :

- La **loi marocaine n°09-08** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
- Le **règlement général européen 2016/679** sur la protection des données qui est entré en vigueur le 25 mai 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- La **loi française n°78-17** du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée ;
- La **loi marocaine n°07-03** sur les infractions liées aux systèmes de traitement automatisé des données ;
- La **loi marocaine n°53-05** relative à l'échange électronique de données juridiques qui précise les règles liées à l'utilisation des moyens cryptographiques pour l'échange de données.

Chacun des pays dans lesquels des entités du Groupe sont implantées dispose de sa propre réglementation en matière de Sécurité des Systèmes d'Information et de protection des données personnelles, qui diffère d'un pays à l'autre.

Les entités du Groupe doivent appliquer des mesures au moins équivalentes aux obligations citées ci- dessus et à la politique du Groupe en matière de Sécurité des Systèmes d'Information et de protection des données personnelles, tout en respectant les obligations locales. Lorsque la réglementation locale impose des obligations complémentaires ou plus strictes, ces dernières doivent également être appliquées.

V. DIFFUSION

La présente Politique Générale de Sécurité des Systèmes d'Information sera diffusée à tout le personnel et devra être communiquée à tout nouvel utilisateur du système d'information d'Intelcia. Elle sera également déposée dans l'Intranet.

Par souci d'adéquation avec le contexte juridique, les besoins technologiques et les exigences métiers d'**Intelcia**, la présente politique sera annuellement revue et mise à jour au regard de son application durant l'année écoulée. Sa revue et sa mise à jour s'imposeront aussi en cas de changement majeur au sein du système d'information d'**Intelcia.**

VI. ROLES ET RESPONSABILITES DANS LE CADRE DE LA MISE EN ŒUVRE DE LA PGSSI

La mise en œuvre de la PGSSI se traduit par l'attribution de responsabilités telles que définies ci-dessous.

VI.1 LA DIRECTION GENERALE

La Direction Générale constitue l'instance décisionnelle quant au pilotage global de la sécurité de l'information. La direction est responsable de l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI et est responsable de :

1. L'établissement d'une politique relative au SMSI;
2. L'assurance que des objectifs et des plans pour le SMSI sont établis;
3. La définition de rôles et de responsabilités pour la sécurité de l'information;
4. La sensibilisation de l'organisme à l'importance de satisfaire aux exigences relatives à la sécurité de l'information et de respecter la politique en matière de sécurité de l'information, à ses responsabilités au titre de la loi et à la nécessité d'une amélioration continue;
5. La fourniture de ressources suffisantes pour l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI;
6. La détermination des critères d'acceptation des risques et des niveaux de risque acceptables;
7. L'assurance que des audits internes du SMSI sont menés;
8. La réalisation de revues de direction du SMSI;
9. Fournir les ressources nécessaires pour établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer du SMSI.

VI.2 LE RESPONSABLE DE LA SECURITE DES SYSTEMES D'INFORMATION (RSSI)

Le RSSI est en charge de s'assurer de la déclinaison de la PGSSI au sein du groupe Intelcia. Le RSSI est habilité à intervenir sur tous les aspects de la sécurité de l'information chez Intelcia. Par des directives administratives, préalablement soumises à la direction générale, il décide, en général, de tout ce qui est nécessaire au fonctionnement efficace du SMSI.

Les principales responsabilités du RSSI inclus :

Etude projets, accompagnement et conseil

- Décliner et contrôler l'application des standards de sécurité adoptés et des politiques définies dans le cadre du Systèmes de Management de la sécurité de l'information (ou SMSI) Intelcia.
- Élaborer et maintenir un programme de gestion des risques de sécurité.
- Proposer les choix en matière de solutions préventives, réactives, organisationnelles et techniques.
- Accompagner les métiers dans la définition de leurs exigences sécurité et dans le choix des services de sécurité en y répondant.

Veille, alerte et sensibilisation :

- Définir et gérer le programme de formation et de sensibilisation à la sécurité de l'information.
- Identifier les exigences sécurité en matière de conformité (mesures juridiques, réglementaires et contractuelles) et définir les actions visant à mettre en œuvre ces exigences.
- Réagir aux incidents sécurité, les suivre et piloter leur analyse, identifier les écarts aux règles de sécurité et apporter l'assistance nécessaire à la résolution de ces incidents.

- Assurer une veille dans le domaine de la sécurité de l'information.

Contrôle interne, Audit et Reporting :

- Assurer un reporting de sécurité aux différentes instances de gouvernance de la sécurité SI, notamment sur les risques encourus et les incidents sécurité, l'état d'avancement des plans d'action et la mise en place de la gouvernance de sécurité du SI.
- Effectuer des contrôles permanents pour s'assurer que les politiques sécurité SI sont appliquées dans les lignes métiers et processus concernés.
- Planifier et effectuer des audits de sécurité réguliers pour l'ensemble des sites d'**Intelcia**, et suivre la mise en œuvre des recommandations des entités de contrôle internes et externes en matière de sécurité du SI.

VI.3 LE DIRECTEUR DES SYSTEMES D'INFORMATION

Le Directeur des Systèmes d'Information d'Intelcia est chargé de :

- Mettre en œuvre les recommandations sécurité nécessaires à la protection des SI issues des plans d'action de sécurité recommandés par le RSSI ou par les entités de contrôles externes.
- Prévoir le budget nécessaire à la mise en œuvre des plans d'action sécurité qui sont affectés à ses équipes.

VI.4 LES RESPONSABLES D'ENTITES SI

Ils veillent à l'intégration des mesures de sécurité nécessaires dans l'exploitation et les projets SI conformément aux politiques de sécurité définies, ils sont responsables de la mise en place et du suivi des plans d'actions sécurité qui leur sont affectés.

VI.5 LES CHEFS DE PROJET SI

Ils définissent explicitement les modalités d'organisation et les moyens techniques pour garantir la sécurité dans leurs projets SI.

Ils contribuent à l'analyse des risques dans les phases en amont des projets SI et s'assurent de la mise en place des actions nécessaires à la réduction des risques liés à la sécurité des SI.

VI.6 LES ADMINISTRATEURS SI

Ils sont acteurs principaux pour le déploiement des mesures de sécurité du SI conformément aux politiques de sécurité définies, contribuent activement aux contrôles des accès aux applications sensibles, et assurent une veille sécurité chacun dans son domaine d'expertise.

VI.7 LES LIGNES METIERS ET LES DIRECTIONS CENTRALES

D'une manière générale, Les lignes métiers doivent saisir le RSSI lors de toute initiative susceptible de modifier la nature et/ou le niveau des risques liés à la SSI, notamment dans les cas suivants :

- lors du lancement de nouvelles offres métiers, de nouveaux produits ou de nouvelles activités ;

- pour toute initiative ou projet d'externalisation et/ou de localisation de services ou d'activités, à l'extérieur comme à l'intérieur du Groupe ;
- lors de la mise en place d'une joint-venture ;
- lors de l'acquisition ou la cession d'activité ou d'entité.

D'une manière spécifique, les rôles et responsabilités des entités ou personnes contributrices à la sécurité SI sont décrits ci-dessous :

- **La Direction des moyens généraux :** Est responsable de la mise en place des mesures de sécurité nécessaires pour assurer la sécurité des accès physiques aux environnements du SI.

- **La Direction des Ressources Humaines** :

  - Effectue des vérifications sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique, s'assure qu'elles sont proportionnées aux exigences métier et aux risques identifiés ;
  - S'assure que les accords contractuels entre les salariés et les freelances précisent les responsabilités de chacun et celles de l'organisation en matière de sécurité de l'information ;
  - Applique les sanctions convenues en cas de non-respect des règles sécurité.

- **La Direction Formation** : Assure les formations adéquates et validées par le RSSI, des collaborateurs en matière de sécurité de l'information.

- **La Direction Communication et Marketing** : Assure la sensibilisation des collaborateurs en matière de sécurité de l'information (affiches, newsletters, etc…) en collaboration avec le RSSI.

- **Le Département juridique** : Assure la veille règlementaire et les aspects contractuels avec les clients et informe le département conformité pour l'analyse d'impact des changements et le respect des règlementations en matière de sécurité des SI.

- **Le Département Achats :** Assure les aspects contractuels et l'intégration des clauses de sécurité (confidentialité, auditabilité et réversibilité) dans les contrats avec les fournisseurs.

- **Le Département conformité et gestion des risques** :
  - Collabore mutuellement avec le RSSI pour la réalisation des audits sécurité et de conformité, pour l'identification des cas de non-conformité aux règles de sécurité, et leurs préconisations.
  - Intègre la composante des risques sécurité SI dans le cadre global de la gestion des risques opérationnels (lutte contre la fraude, continuité d'activité métier, contrôle permanent, etc…)

  Le RSSI est le correspondant privilégié des responsables des risques opérationnels pour ce qui concerne les risques opérationnels se rapportant à la SSI.

- **Le Département méthodes et processus** : Prend en charge la centralisation et la diffusion des documents liés à la sécurité de l'information.

- **Les responsables hiérarchiques** : S'assurent que chaque personnel placé sous leurs responsabilités a été informé des règles à respecter et des comportements à adopter en matière de sécurité du SI.

- **L'ensemble du personnel** : Respecte les lois, règlements, le devoir de réserve et contrats, ne contourne pas les dispositifs de sécurité mis en place et informe sa hiérarchie de tout incident, anomalie et infraction par rapport aux règles de sécurité en vigueur.

VII. INSTANCES DE PILOTAGE

VII.1 Comité Directeur de Sécurité

VII.1.1 Objectifs du CDS

- Aligner le SMSI avec les objectifs et la stratégie d'Intelcia.
- Suivre les indicateurs de sécurité des systèmes d'information.
- Etablir et veiller au suivi du plan d'action.

VII.1.2 Pilotage

Le Directeur Général préside le Comité Directeur de sécurité.

VII.1.3 Missions du CDS

Le **comité directeur de la sécurité** constitue l'instance décisionnelle. Il a pour fonction de :

- Effectuer la revue de direction annuelle.
- Déterminer la stratégie et les objectifs annuels du SMSI.
- Approuver les projets stratégiques afférents à la sécurité d'information.
- S'assurer de la disponibilité des ressources nécessaires au bon fonctionnement du SMSI.
- S'assurer de la prise en compte des valeurs organisationnelles d'**Intelcia** et de ses objectifs stratégiques dans le processus de gestion de la sécurité de l'information
- Suivre les incidents majeurs liés à la sécurité de l'information.

VII.1.4 Membres du CDS

	Membres
A minima	- Directeur Général - Directeur des systèmes d'information - Directeur des moyens généraux - Directeur Qualité - Responsable conformité et gestion des risques - Data Protection Officer (DPO) - Responsable de la Sécurité des Systèmes d'Information

Selon le besoin, d'autres entités peuvent faire partie de ce comité.

VII.1.5 Fréquences de réunions et livrables

Le comité Directeur de sécurité se réunit une fois par an ou à la demande du Directeur Général.

Un compte rendu doit être rédigé à chaque rencontre et communiqué à tous les membres.

VII.2 Comité Opérationnel de sécurité

VII.2.1 Objectif du COS

Assurer le maintien en condition opérationnelle du SMSI.

VII.2.2 Missions du COS

Le Comité opérationnel de la sécurité a pour principale mission de s'assurer que le SMSI répond efficacement aux besoins des processus métiers du groupe Intelcia en termes de sécurité :

- Assurer le déroulement efficace des opérations du SMSI.
- Promouvoir la cohérence de la sécurité de l'information dans l'organisme.
- Gérer les problématiques de sécurité de l'information et proposer des solutions aux non-conformités.
- Piloter et suivre la mise en œuvre des plans d'action de sécurité et l'implémentation des actions correctives qui surgissent de l'analyse du risque.

VII.2.3 Membres du COS

	Membres
A minima	- Directeur des systèmes d'information. - Responsables des entités SI. - Responsables des moyens généraux. - Responsable de la Sécurité des Systèmes d'Information

Selon le besoin, d'autres entités peuvent faire partie de ce comité.

VII.2.4 Fréquence des réunions et livrables

Le comité opérationnel de sécurité se réunit une fois par semestre.

Un compte rendu doit être rédigé à chaque comité et communiqué à tous les membres.

VIII. CORPUS DOCUMENTAIRE DE SECURITE DES SYSTEMES D'INFORMATION

La PGSSI définit le cadre général de l'organisation et de la gouvernance de la sécurité de l'information et s'appuie sur la déclinaison des politiques thématiques, des procédures, des guides et des chartes liés au domaine de la sécurité des systèmes d'information.

Les « Politiques thématiques de sécurité SI » sont des Directives traitant de domaines spécifiques de la SSI au niveau du Groupe ;

Les «Procédures liées à la sécurité SI » décrivent les rôles et responsabilités de chaque acteur impliqué dans un domaine impactant la sécurité SI ;

Les « Guides de sécurité SI » sont des documents techniques contenant des dispositions venant en support d'une Politique de sécurité. Il est obligatoire de s'y conformer dans le domaine considéré ;

Les « Chartes » décrivent les règles de sécurité à respecter par les utilisateurs des ressources SI. Un engagement nominatif doit être signé à cet effet.

Ci-dessous une liste des politiques thématiques de sécurité SI qui sont formalisées dans des documents relatifs à chacune d'elle.

Politique thématique sécurité	Description
Sécurité réseaux	Directives et recommandations de sécurité permettant de garantir la disponibilité des réseaux et des équipements qui y sont connectés ; L'intégrité et la confidentialité des échanges via les réseaux ainsi que les données hébergées sur les équipements réseaux ; La traçabilité de l'ensemble des accès aux ressources des réseaux.
Sécurité des postes de travail et terminaux mobiles	Directives et recommandations de sécurité à appliquer dans la conception, le déploiement et la gestion des postes de travail et des terminaux mobiles.
Classification et manipulation des actifs	Enoncé de règles de classification de sécurité et proposition d'une aide à la classification de la sécurité des informations d'Intelcia en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée.
Contrôle d'accès et gestion des habilitations SI	Définition des principales règles pour la maitrise des accès logiques aux systèmes d'information, l'attribution des habilitations respectant le principe du moindre privilège.
Sécurité physique et environnementale	Définition des principales règles pour la maitrise des accès physiques aux zones sensibles hébergeant les systèmes d'information.
Sécurité des mots de passe	Description des dispositions à prendre en termes de gestion des mots de passe des utilisateurs.
Cryptographie et gestion des clés	Description des règles nécessaires à la génération, la conservation, la distribution, la modification et la destruction sécurisées des clés utilisées pour le cryptage des données.
Sauvegarde et de restauration des données	Fixation des règles et contrôles nécessaires aux opérations de sauvegarde, d'externalisation des bandes et de restauration des données.
Gestion des vulnérabilités techniques et des correctifs de sécurité SI	Définition des règles et principes directeurs relatifs au processus de gestion des vulnérabilités et des correctifs de sécurité.
Protection antivirale	Fixation des règles de sécurité pour une protection efficace contre les codes malveillants.
Développement sécurisé des applications	Directives de sécurité de développement des applications pendant tout le cycle de développement.
Surveillance et de journalisation du SI	Définition d'un cadre pour enregistrer les événements de sécurité, détecter les actions et opérations anormales et garantir la sécurité des traces des opérations réalisées sur les systèmes d'information.
Sécurité Fournisseurs	Définition des exigences de sécurité des fournisseurs et l'engagement de ces derniers à respecter la politique de sécurité SI.

GLOSSAIRE

TERME	DEFINITION
Confidentialité	Propriété selon laquelle une information ne peut être divulguée ou rendue accessible à des individus, filiales ou processus n'ayant pas à connaître cette information, ou non autorisés.
Disponibilité	Propriété d'une information d'être accessible et utilisable à la demande d'une personne ou d'une filiale autorisée dans les délais impartis.
Intégrité	Propriété assurant qu'une information – ou un processus automatisé de traitement de cette information – n'a pas été modifiée, altérée ou détruite de façon non autorisée.
Traçabilité	Propriété d'être en mesure de prouver qu'une action ou un événement relatif à l'information a eu lieu. Elle est caractérisée par un niveau de qualité de mémorisation des différentes actions liées à l'utilisation des informations manipulées (par exemple, à travers l'existence et l'archivage de « pistes d'audit »).
Incident de sécurité (de l'Information)	Evènement de sécurité, isolé ou multiple, indésirable ou inattendu, entrainant une probabilité significative de mettre en péril des opérations Métier et/ou porter atteinte à la sécurité de l'information.
Information	Dans le contexte de ce document, nous considérons comme « information » : • Toute donnée pertinente dont la collecte, le traitement, l'interprétation et l'utilisation concourent à la réalisation d'une mission (métier) ; • Tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.
Patrimoine Informationnel	Cf. Information
RSSI	Responsable Sécurité des Systèmes d'Information
SI	Système d'Information
SMSI	Système de Management de la sécurité de l'Information : Ensemble de politiques, procédures et dispositifs organisationnels et techniques basés sur les risques pour la protection de la confidentialité, de l'intégrité et de la disponibilité du patrimoine informationnel
SSI	Sécurité des Systèmes d'Information
PGSSI	Politique Générale de Sécurité des Systèmes d'Information
CDS	Comité Directeur de Sécurité
COS	Comité Opérationnel de Sécurité

Date et Signature du Directeur Général :

Date	**30/06/2021**
Signature	**Youssef EL AOUFIR**