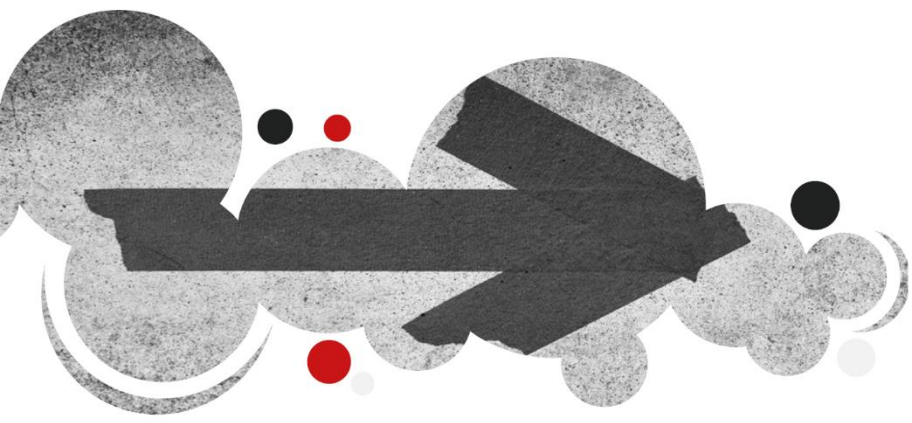
PGSI - Politique Générale de Sécurité de l'Information ITS Integra

Référence du document :	ITS-Integra-PGSI-Politique-Generale-Securite
Date d'émission :	10/03/2026
Validation du document :	1 an



SOMMAIRE

1. Les grands principes

1.1. Contexte de la sécurité du système d'information chez ITS Integra

Face à la montée des cyberattaques, de l'utilisation du Cloud ou encore des demandes de transformation digitale, nous plaçons la sécurité des données et des infrastructures IT au cœur des enjeux stratégiques de ITS Integra, notamment pour répondre aux besoins de protection des entreprises sur leur Système d'Information dans des secteurs très exigeants comme la Santé. Ainsi, la préservation de la sécurité informatique de nos clients et donc de leur image et notoriété est un enjeu stratégique capital pour ITS Integra.

En cohérence avec ses ambitions et celles de nos clients, nous avons déployé une Politique de Sécurité de son Système d'Information (PSSI) répondant à nos engagements en termes de disponibilité, intégrité, confidentialité et traçabilité. Les règles de sécurité de cette politique sont appliquées par l'ensemble des collaborateurs et intervenants de ITS Integra.

Notre Système de Management de la Sécurité de l'Information (SMSI), déployé sur nos activités d'hébergement, d'infogérance et de Cloud Computing, nous assure une maîtrise des performances de notre SI tout en satisfaisant aux demandes de nos clients.

L'enjeu de notre SMSI est de nous assurer que nos activités répondent à nos engagements clients en matière de disponibilité, intégrité, confidentialité et traçabilité et satisfaire leurs attentes dans la contribution de ITS Integra dans leur développement économique. Notre SMSI nous assure également de la conformité de notre organisation avec l'ensemble des exigences légales et réglementaires applicables, ainsi qu'avec les référentiels ISO/IEC 27001:2022 et HDS.

Les enjeux et les engagements de ITS Integra, décrits ci-après, sont définis et réévaluées périodiquement en Revue de Direction. Leurs indicateurs sont définis et suivis annuellement dans le tableau de pilotage du SMI.

1

Enjeu
Renforcer la sécurité des Systèmes d'Information

Engagement
Atteindre un niveau de sécurité homogène, robuste et auditable

2

Enjeu
Garantir la résilience et la disponibilité des plateformes Cloud

Engagement
Améliorer la continuité de service et réduire les incidents majeurs

3

Enjeu
Industrialiser les environnements

Engagement
Fiabiliser les déploiements, réduire la charge et améliorer la qualité

4

Enjeu
Maintenir les compétences clés en interne

Engagement
Sécuriser la continuité opérationnelle et renforcer l'efficience

5

Enjeu
Assurer la conformité aux cadres réglementaires et normatifs

Engagement
Maintenir les certifications du SMI, protéger les DSCP et anticiper les évolutions réglementaires

6

Enjeu
Préserver la satisfaction client et renforcer la transparence opérationnelle

Engagement
Consolider la confiance et fidéliser un marché de plus en plus exigeant

7

Enjeu
Maintenir une trajectoire de conformité liée au Cloud de confiance

Engagement
Développer des offres de Cloud souverain et obtenir des certifications

1.2. Revues de la politique générale de sécurité

La PGSI de ITS Integra est révisée à minima une fois par an. Elle peut être également révisée en cas de changements significatifs. Dans ce cas, la version modifiée sera communiquée à l'ensemble des parties prenantes pertinentes, afin de les informer des dits changements.

Les révisions sont à l'initiative du RSSI de ITS Integra, en collaboration avec les propriétaires des actifs identifiés, et sont proposées à la Direction Générale.

La mise en place d'une nouvelle version, majeure ou mineure, doit être validée par la Direction Générale.

1.3. Domaine d'application du SMSI

Le SMSI de ITS Integra est certifié ISO/IEC 27001:2022 et HDSv2 sur le périmètre :

« INFORMATION SECURITY MANAGEMENT SYSTEM FOR HOSTING, HEALTH DATA HOSTING, CLOUD COMPUTING, MANAGED SERVICES FOR ASPLENIUM & ITS INTEGRA ».

Une déclaration d'applicabilité nous permet de présenter les dispositions établies pour répondre aux mesures de l'annexe A de l'ISO/IEC 27001:2022 et de la HDSv2 conformément à nos certifications.

Précisément, le SMSI, applicable au périmètre ITS Integra, n'exclut aucune clause de la norme ISO/IEC 27001:2022. Le chapitre développement externalisé de l'annexe A de l'ISO/IEC 27001:2022 (A.8.30), non pratiqué chez ITS Integra, est lui exclus du périmètre, de même que les chapitres HDSv2 relatifs à l'accès à distance depuis un pays hors Espace Economique Européen (EEE) et à la législation d'un pays tiers (EXI 29 et EXI 30).

Les postes destinés à l'activité « Centre de Services » fournis par les clients sont soumis à la politique sécurité des clients et de fait exclus du périmètre du SMSI ITS Integra. Les activités spécifiques de la Direction Solutions sont également exclues du périmètre de certification et du SMSI ITS Integra.

Géographiquement, le périmètre du SMSI comprend l'ensemble des Data Center et des sites de bureaux en France.

Le SMSI interagit avec une entité externe ITS Group. Cette interface fait l'objet d'une Convention de Services et de contrôles de sécurité.

Le bon fonctionnement du SMSI dépend des services suivants : connectivité internet par les transitaires (OPENTRANSIT, COLT et FRANCEIX), fournisseur de fibre noire (SIPARTEC), fournisseur de Data Center (DIGITAL REALTY), fournisseurs de services Cloud (AZURE, O365 et OVH).

Le périmètre du SMSI inclus également la protection des données de santé à caractère personnel dans le cadre de l'activité d'hébergement de données de santé. En effet, ITS Integra est certifié Hébergeur de Données de Santé (HDSv2) sur l'ensemble des périmètres du référentiel, au sens des dispositions de l'article L.1111-11 du Code de la santé publique, et est autorisée par les services compétents à réaliser des prestations d'hébergement de données de santé à caractère personnel. Ces prestations d'hébergement comprennent le cas échéant des prestations permettant l'accès direct du patient aux applications et à ses données de santé à caractère personnel. Tous les moyens et processus utilisés dans les activités certifiées sont inclus dans le périmètre, y compris la sauvegarde et les transferts de supports d'information.

Dans le cadre de l'activité d'Hébergement de Données de Santé, les activités suivantes sont certifiées :

1. La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
3. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
4. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
5. L'administration et l'exploitation du système d'information contenant les données de santé ;
6. La sauvegarde de données de santé.

2. S'engager : le maître mot

Basée sur le respect de l'ISO/IEC 27005:2022, l'appréciation des risques en matière de sécurité de l'information se déroule à minima annuellement et est pilotée par le Responsable Sécurité des Systèmes d'Informations (RSSI). Cette analyse peut également être déclenchée en cas de changements impactant, tant organisationnels que techniques.

Les résultats sont présentés en Revue de Direction et la décision, quant au seuil d'acceptabilité des risques, est décidée puis annoncée dans la lettre d'engagement rédigée par le dirigeant, à l'attention de toutes les parties prenantes.

De ces résultats en découlent des actions qui sont identifiées et validées dans le Plan de Traitement des Risques (PTR) garant du suivi et du déroulement des initiatives en matière de réponse à l'appréciation des risques.

Une veille réglementaire et technologique précise assurée par le pôle RSSI, ainsi que la collaboration avec des organismes tels que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ou encore des entreprises privées, permettent la mise en œuvre des actions supplémentaires, de les piloter et de les contrôler dans le temps.

Ainsi, les mesures instaurées sont applicables à différentes activités :

- Accès logiques et physiques,
- Charte informatique,
- Classification et transmission de la donnée,
- Contrôle des accès aux données,
- Identifiant unique et gestion des privilèges,
- Implication du personnel,
- Management des actifs,
- Usage réseau.

La force de notre engagement réside dans la globalisation des pratiques sécurité, quel que soit le périmètre même non certifié.

2.1. Gouvernance du SMSI

Afin de maintenir un suivi des performances du SMSI de ITS Integra et d'alimenter la démarche d'amélioration continue, plusieurs comités ont été instaurés à fréquence planifiée avec des objectifs différents, comme présentés dans le tableau ci-dessous.

	Revue de Direction SMI	Comité SMI	Audit interne	Audit externe
Objectifs SMSI	Validation appréciation des risques Revue stratégique de l'orientation de la politique sécurité et de la pertinence du SMSI	Suivi des actions du SMI Suivi des indicateurs	Identifier écarts, points d'amélioration et opportunité pour amélioration de l'efficacité et efficience des process	Evaluation du système de management en vue du maintien ou du renouvellement des certifications
Fréquence	Annuelle	Mensuelle	Annuelle	Annuelle
Eléments d'entrée	CR d'audits interne et externe Appréciation des risques Plan de Traitement des Risques (PTR)	Suivi avancements des plans d'action et PTR Revue KPI Remontées non-conformité, écarts, amélioration	Référentiel ISO/IEC 9001:2015, ISO/IEC 27001:2022, HDSv2 Revue de Direction Processus	Périmètre de certification Programme d'audit Documents internes
Eléments de sortie	Revue des actions Revue des KPI Définition des objectifs Risques résiduels PTR actualisé Seuil d'acceptabilité Evolution du SMSI	Mise à jour documentaire Plan d'actions à jour Réclamations ou vigilances internes	Visibilité sur l'efficacité et efficience activités / processus Axes d'amélioration définie	CR Délivrance ou maintien certificat Préconisations d'amélioration Actions correctives éventuelles pour mise en conformité
Pilote	RSSI Responsable Qualité	RSSI Responsable Qualité	Auditeur interne	Auditeur externe
Membres ITS Integra à minima *Toute personne supplémentaire identifiée pourra être conviée*	Responsable Qualité RSSI Direction ITS Integra Pilote des processus	Responsable Qualité RSSI Direction ITS Integra Pilote des processus	Responsable Qualité RSSI Direction ITS Integra Pilote des processus	Responsable Qualité RSSI Direction ITS Integra Pilote des processus

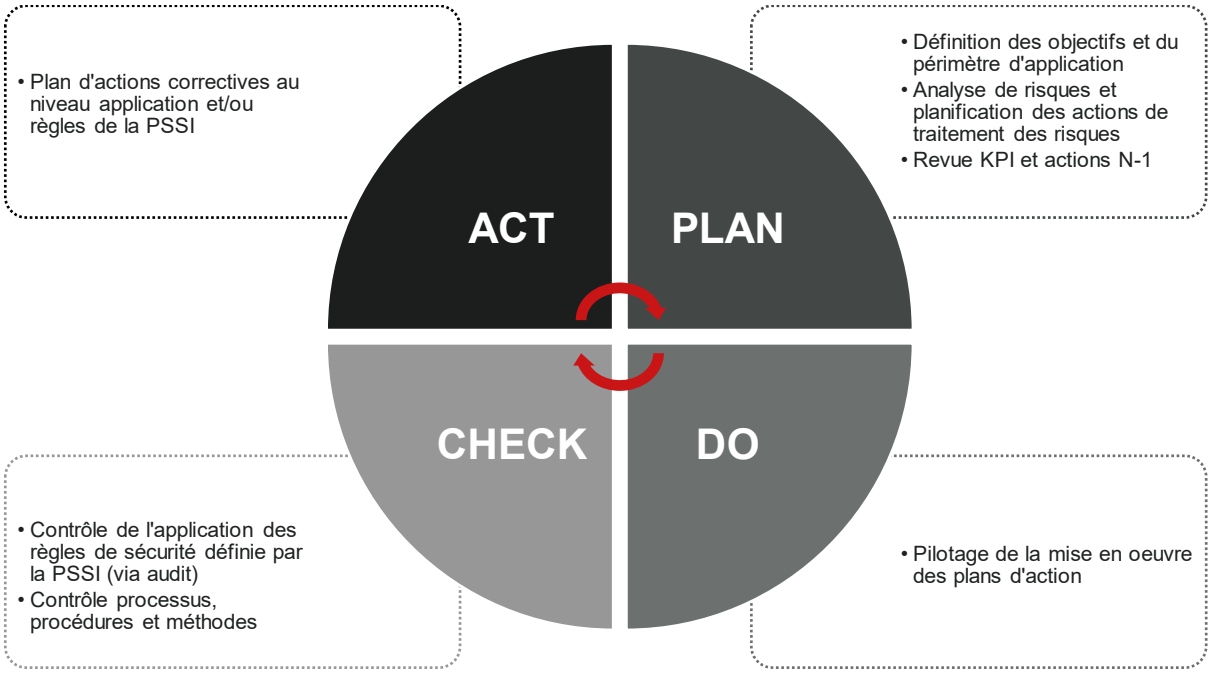
2.2. Amélioration continue

Le Système d'Information de ITS Integra fait l'objet d'une analyse de risques permettant, entre autres une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue et permet de maintenir une maîtrise des risques identifiée.

Les éléments constitutifs du SMSI (processus, procédures, etc.) sont appelés à évoluer dans l'optique d'une amélioration continue.

La pertinence, l'adéquation et l'efficacité du SMSI dans le contexte de l'entreprise sont évalués à fréquence planifiée par le biais notamment d'une gouvernance en matière de sécurité de l'information, décrite dans le sous-chapitre précédent.

Ainsi, la démarche d'amélioration continue du SMSI de ITS Integra s'articule de la manière suivante :



2.3. Rôles et responsabilités et autorités au sein de l'organisation

La Direction de ITS Integra a nommé un RSSI pour s'assurer de la conformité du SMSI aux exigences de la norme ISO/IEC 27001:2022 et HDSv2. Le RSSI s'appuie sur des instances internes pour l'assister dans ses missions. Les rôles et responsabilités ont été définis et communiqués au sein de l'organisation. Le RSSI rend régulièrement compte à la Direction de la performance du SMSI.

Chaque collaborateur est informé qu'un non-respect de la PGSI ou des politiques associées peut entraîner une suspension des certifications avec un fort impact sur l'activité de l'entreprise, pour cette raison, des sanctions seront appliquées conformément au règlement intérieur en cas de violation des règles de sécurité. Les sanctions peuvent aller jusqu'au licenciement pour fautes lourdes en fonction de la gravité de la situation

Le tableau ci-dessous illustre les grandes catégories de rôles et responsabilités au sein du SMSI de ITS Integra. La liste exhaustive des rôles et responsabilités du SMSI est présente dans le référentiel associé.

	Rôles et responsabilités
Direction Générale	• Porter la responsabilité de la sécurité du SI de ITS Integra, • S'engager sur la disponibilité des ressources de la collectivité à mobiliser sur la Sécurité du Système d'Information.
RSSI	• Etablir et mettre en œuvre le Plan de Traitement des Risques, • Animer la gouvernance de la Sécurité du Système d'Information, • S'assurer du bon déploiement de la PSSI, • Vérifier que les règles à suivre sont bien appliquées, • Mettre en place les programmes de formation et de sensibilisation, • Réaliser les revues d'analyse de risque, • Se tenir informé de la réglementation en matière de sécurité de l'information, • Être garant de la gestion documentaire lié à la Sécurité du Système d'Information.
Responsable Qualité	• Formaliser les documents lié au SMSI, • Participer au suivi des indicateurs.
DPO	• Informer, sensibiliser et diffuser une culture de compliance sur le sujet de la protection des données personnelles, en particulier aux équipes techniques pouvant interagir avec les données de santé dans le cadre d'une TMA, • Participer à la mise en œuvre de la procédure d'exercice des droits et de notification des violations de données personnelles en cas d'un incident interne ou client impliquant une potentielle violation de données personnelles.
DSI	• Soutenir l'action du RSSI, • Gérer les IN/OUT/MOVE et le parc bureautique.
Manager	• Soutenir l'action du RSSI, • Vérifier la bonne application des règles à suivre.
Equipes Techniques	• Déployer les mesures de sécurité dans leur domaine respectif

3. Systématiser la sécurité auprès de tous

La charte informatique (Charte ITCom), ainsi que l'engagement de confidentialité, permettent à ITS Integra d'impliquer les collaborateurs dans la démarche de sécurité de l'information globale. Au-delà du périmètre certifié, ITS Integra fait le choix également de diffuser les bonnes pratiques à l'ensemble de ses collaborateurs.

La charte informatique constitue un élément d'engagement et de responsabilisation des salariés. Ce document garantit que le collaborateur connait les règles générales à appliquer, afin de protéger l'accès aux données à travers le matériel qui lui est confié, mais aussi afin de garantir la préservation des dispositifs de sécurité en place et la valeur de la confidentialité de l'information.

L'engagement de confidentialité, comme la charte informatique, est présenté lors de la signature du contrat de travail, en annexe. L'engagement de confidentialité peut être transmis sur demande aux clients lors des audits.

Par ailleurs, les collaborateurs sont régulièrement conviés à des ateliers dans le but de les informer et de les sensibiliser aux nouveaux outils de sécurité, à l'évolution des exigences réglementaires et aux bonnes pratiques. La newsletter interne est également un support essentiel de la communication sur les aspects sécurité. Enfin, le plan de formation annuel permet de répondre aux besoins des collaborateurs en termes de compétences et d'anticiper les évolutions de l'environnement.

Chaque collaborateur est informé qu'un non-respect de la PGSI ou des politiques ou procédures associées peut entraîner une suspension des certifications avec un fort impact sur l'activité de l'entreprise, pour cette raison, des sanctions seront appliquées conformément au règlement intérieur en cas de violation des règles de sécurité.

4. Maintenir une architecture résiliente

Lors de l'appréciation des risques, une liste des actifs est dressée selon le périmètre technique certifié. Il est précisé pour chaque actif son propriétaire, et la politique applicable à son utilisation.

De plus, chaque donnée est soumise à une classification, qui a pour but de définir les conditions de manipulation, de criticité, selon les exigences légales. Pour les données contenues dans des supports amovibles, tels que les ordinateurs portables, une procédure est mise en place afin de déterminer précisément les conditions de mise à disposition et de transfert.

Les politiques essentielles de sécurité sont :

- Patch Management,
- Antivirus,
- Sauvegardes,
- Gestion des traces,
- Gestion maintenance matériel,
- Gestion du réseau,
- Contrôles accès aux données,
- Contrôles accès logiques,
- Contrôles accès physiques,
- Normes nouvelles applications,
- Normes de développement,
- Gestion des incidents,
- Gestion de la capacité,
- Gestion des ressources humaines,
- Gestion de la sécurité dans les projets.

Les différentes politiques sont décrites dans le document de Politique de Sécurité des Systèmes d'Information (PSSI).

5. Garantir notre continuité de service

Conformément aux exigences ISO/IEC 27002:2022 et aux besoins internes, ITS Integra procède régulièrement à la revue et à l'audit technique de son infrastructure. Ces contrôles permettent de maîtriser au mieux la conformité avec ce qui a été défini et est connu de tous notamment dans le cadre du Plan de Continuité d'Activité (PCA).

Pour ce faire, ITS Integra a défini une organisation et des modes opératoires associés ayant pour but de garantir la survie de l'entreprise lors un sinistre important. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

Lors de l'appréciation des risques réalisée dans le cadre de la norme ISO/IEC 27001:2022, il a été identifié trois types de risques nécessitant la mise en place du Plan de Continuité.

5.1.1. Perte ou indisponibilité d'un site physique

Ce risque regroupe l'ensemble des problèmes liés aux bâtiments. Le risque peut être temporaire (perte de sources d'énergie) ou définitif dans le cas d'une destruction du bâtiment. Nous distinguons également deux types de bâtiments : les Data Centers d'une part et les bureaux d'autre part.

5.1.2. Indisponibilité d'un nombre important de salariés

Il s'agit de l'indisponibilité d'un nombre important de salariés ou dans l'incapacité de se rendre au travail. Cette indisponibilité pourrait avoir des origines diverses comme des grèves massives, une pandémie virale, etc.

5.1.3. Perte ou corruption d'un service vital (core service)

Le bon fonctionnement des services de cœurs de réseaux étant vital, ils entrent dans le PCA, afin que des mesures de redondance adéquates soient mises en place.

Integra

VOTRE SATISFACTION AU CŒUR DE NOS ENGAGEMENTS

RESPONSABILITÉ • SÉCURITÉ • SOUVERAINETÉ

contact@itsintegra.com

+33 (0)1 78 89 35 00
42 rue de Bellevue
92100 Boulogne Billancourt

http://www.itsintegra.com

Suivez toute l'actualité