PREMIER MINISTRE

Liberté
Égalité
Fraternité

Direction Interministérielle du Numérique

Politique du Système de Management de la Sécurité de l'Information

–

FranceConnect

– NON PROTEGE –

Version 1.4

Propriétés du document

	Identité	Date
Rédacteur	Laurent BARRAT	10/12/2025
Contrôleur	Linda DEBERNARDI	16/12/2025
Approbateur	Florian DELEZENNE	15/01/2026

Historique des versions

Version	Résumé des modifications	Modifié par	Date
v0.1	Initialisation du document	Laurent BARRAT	04/09/2024
v1.0	Version finale	Laurent BARRAT	24/09/2024
v1.1	Revue des indicateurs et corrections de coquilles. Ajout des indicateurs demandés par l'auditeur.	Laurent BARRAT	13/12/2024
V1.2	Ajout des précisions sur la direction. Ajout de la clause sur les enjeux climatiques	Laurent BARRAT	18/12/2024
V1.3	Modification de l'indicateur ST02-COMITOLOGIE Ajout des indicateurs : ○ OP06-PCA/PRA_CC ○ OP07-REST Révision des indicateurs : ○ ST05-PARTENAIRES-NB ○ ST06-PARTENAIRES-CO Ajout des objectifs (seuil satisfaisant/ insatisfaisant) pour tous les indicateurs Ajout de la Gestion documentaire (§6.2)	Laurent BARRAT	19/03/2025
V1.4	Restructuration des chapitres. Ajout d'éléments synthétiques concernant le fonctionnement du SMSI, notamment via l'ajout des chapitres : ○ Parties intéressées par le SMSI (§ 4.4) ; ○ Attentes des parties intéressées (§ 4.4) ; ○ Audits du SMSI (§ 6.3.2) ; ○ Instances de gouvernance (§ 6.3.3) ; ○ Amélioration (§ 6.4) ;	Marceau VIENNE	25/06/2025
	Relecture et prise en compte des décisions de la revue de direction de mars 2025. Réécriture du §6.2 Documentation du SMSI.	Laurent BARRAT	22/07/2025
	Ajout des enjeux climatiques des hébergeurs. Suite à relecture par le responsable produit, correction : ○ Contexte et organisation	Laurent BARRAT	10/12/2025

	○ Présentation des modes d'authentification ○ Objectif de FranceConnect+ ○ Marchés ○ FI ○ Exigences		
	Modifications du l'organisation suite relecture par le Chef de département afin de prendre en compte la réorganisation de la DINUM.	Laurent BARRAT	15/01/2026

Liste de diffusion

Destinataire	Poste	Société
L'ensemble de l'équipe FranceConnect.		
Parties intéressées du SMSI (cf. § 4.4.1 Liste des parties intéressées)		

Table des matières

Glossaire

Acronyme	Signification
AIPD	Analyse d'Impact sur la Protection des Données
ANSSI	Agence nationale de la sécurité des systèmes d'information
DSAF	Direction des Services Administratifs et Financiers
eIDAS	Electronic IDentification And Signature
FD	Fournisseurs de Données
FI	Fournisseurs d'Identité
FS	Fournisseurs de Services
PSSI	Politique de sécurité des systèmes d'information
PSSIE	Politique de Sécurité des Systèmes d'Information de l'État
PTR	Plan de Traitement des Risques
RSMSI	Responsable SMSI
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'information
SMSI	Système de management de la sécurité de l'information
SPM	Services du Premier Ministre
SSI	Sécurité des Systèmes d'Information

Note : le pronom personnel masculin est largement utilisé dans ce document (et de manière plus générale dans l'ensemble des livrables du SMSI) afin d'en simplifier sa lecture et réduire le cycle des mises à jour. Il en est de même pour le genre des fonctions (directeur, chef, etc.) et peuvent à tout moment être remplacés par leur équivalent féminin pour s'adapter à l'organisation actuelle de la DINUM.

1. ENGAGEMENT DE LA DIRECTION

L'application opérationnelle de la politique de notre système de management de sécurité de l'information – SMSI – n'est possible que par l'engagement des collaborateurs à contribuer et à promouvoir la sécurité au sein de leurs activités quotidiennes.

La Direction ainsi que l'ensemble des responsables de la DINUM s'engagent à mener, à soutenir et à examiner cette politique et ses objectifs et à améliorer en permanence son système de management.

Notre responsable du SMSI – RSMSI, en toute indépendance, se porte garant devant la Direction du bon fonctionnement du SMSI par ses conseils éclairés, sa maîtrise des opérations, sa proactivité et sa réactivité face aux menaces, la pratique d'une veille technologique permanente et l'adaptation des activités en conséquence.

Je lui assure mon plein support et m'engage à libérer les ressources nécessaires pour maintenir et développer notre SMSI.

Je demande à l'ensemble du personnel de souscrire à cette politique en continuant à s'impliquer personnellement dans la voie de la Sécurité de l'Information, en mettant en œuvre intégralement les dispositions du SMSI et en apportant entière collaboration au RSMSI dans ses missions.

La Direction,

Date et signature

Signature
numérique de
SCHAER STEPHANIE
Date : 2026.03.10
13:06:21 +01'00'

2. POLITIQUE DU SMSI

2.1. OBJET DU DOCUMENT

Ce document démontre l'engagement de la Direction Interministérielle du Numérique (DINUM) à la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) pour le système d'information FranceConnect. Dans la suite du document, le terme « SMSI FranceConnect » fait référence au périmètre défini sur les systèmes d'information FranceConnect, FranceConnect+ ainsi que le Nœud eIDAS français.

Ce document définit la méthodologie utilisée afin de déployer et maintenir une démarche de sécurité conforme aux orientations de la DINUM, incluant les exigences « métier » des Administrations de l'État.

Il s'agit de faire appliquer les règles de sécurité obligatoires ainsi que les recommandations de sécurité concernant l'échange et à la diffusion des informations relatives à la sécurité dans le périmètre défini.

La Politique du SMSI de FranceConnect doit répondre aux attentes des parties intéressées et au contexte d'interopérabilité de FranceConnect aux niveaux national et européen. À ce titre, elle :

- précise le domaine d'application du SMSI ;
- définit les orientations générales et les grands principes en matière de sécurité de l'information ;
- rappelle les principales exigences légales, règlementaires, contractuelles du SMSI ;
- présente l'organisation dévolue au management de la sécurité ;
- liste les principaux documents applicables ;
- justifie la mise en œuvre de procédures de fonctionnement du SMSI.

Ce document s'adresse aux acteurs et responsables du Système d'Information de FranceConnect. Afin d'être accessible à toutes les parties intéressées et tous les acteurs impliqués, cette politique est consultable sur demande. Elle est donc destinée au personnel de la DINUM, aux prestataires et partenaires impliqués dans le SMSI FranceConnect.

Pour l'atteinte des objectifs du SMSI, la sécurité de l'information est fondée sur les principes suivants :

- la confidentialité : les données et les systèmes d'information doivent être protégés contre l'accès non autorisé ou la divulgation non autorisée et en particulier les données sensibles, dont les données de usagers ;
- l'intégrité : les données et les systèmes d'information doivent être protégés contre les modifications non autorisées ou les altérations ;
- la disponibilité : les données, les systèmes d'information et les services opérés doivent être accessibles et disponibles pour les utilisateurs ;
- la responsabilité : chaque agent est responsable de la sécurité de l'information et doit prendre des mesures pour la protéger ;
- le respect des lois et réglementations en vigueur sur la protection des données et la sécurité de l'information ;

2.2. CHAMP D'APPLICATION DU DOCUMENT

Ce document s'applique au périmètre du SMSI FranceConnect.

2.3. RESPONSABILITES ET REVUE DU DOCUMENT

La présente politique est approuvée par la direction et fait l'objet d'un réexamen annuel par le RSMSI.

Celle-ci sera adaptée chaque fois que nécessaire, afin qu'elle soit en adéquation permanente avec la philosophie, les objectifs, les activités, les évolutions technologiques, ainsi que les nouveaux risques et changements juridiques.

2.4. CLASSIFICATION DU DOCUMENT

Ce document est classifié « Non-protégé ».

3. CONTEXTE DE L'ORGANISATION

La DINUM créée par le décret du 25 octobre 2019 est un service du Premier ministre, placé sous l'autorité conjointe du Premier ministre et du ministre chargé de l'action publique.

La DINUM a la charge de la transformation numérique de l'État au bénéfice du citoyen comme de l'agent, sous tous ses aspects : modernisation du système d'information de l'État, création de services publics innovants pour les citoyens, qualité des démarches en ligne, gouvernement ouvert, etc.

La DINUM accompagne les ministères dans leur transformation numérique, conseille le gouvernement et développe des services et ressources partagées comme le Réseau interministériel de l'État, FranceConnect, data.gouv.fr ou api.gouv.fr.

La DINUM comprend six départements :

- le département « Expertise technique et ressources » (ETR) définit, en lien avec les directions du numérique ministérielles, les réglementations et standards techniques du numérique de l'Etat. Il assure le contrôle des grands projets numériques, le dialogue et la collaboration avec les collectivités territoriales ainsi que le suivi de la dépense numérique de l'Etat et de sa stratégie d'achat. Il soutient les autres départements de la DINUM en matière budgétaire, juridique et de communication dans un souci de simplification de processus et d'efficience ;
- le département « Accompagnement de services numériques » (ASN) anime le programme beta.gouv.fr et accompagne les administrations pour faire réussir leurs projets numériques, en maximiser l'impact et en améliorer le design ainsi que l'accessibilité ;
- le département « IA dans l'Etat » (IAE) pilote et met en œuvre la stratégie de l'Etat en matière d'intelligence artificielle au service de l'action publique, en favorisant les mutualisations et en mettant notamment à disposition des administrations un socle technique commun ;
- le département « Infrastructures et services opérés » (ISO) construit et opère des infrastructures et services d'usage partagé, et notamment le réseau interministériel de l'Etat (RIE), dont la stratégie de résilience et de sécurité est définie conjointement avec le secrétariat général de la défense et de la sécurité nationale (SGDSN) ;
- le département « Opérateur de produits interministériels » (OPI) construit, met à disposition et opère des services numériques d'usage partagé, notamment un service de fédération d'identités électroniques, une plateforme numérique de mise à disposition de données administratives et des outils numériques à destination des agents publics. Il définit également la stratégie interministérielle de déploiement de ces services et coordonne l'appui de la DINUM à l'open source et aux communs numériques ;
- le département « RH de la filière numérique de l'Etat » (RHN) soutient le développement des compétences de l'Etat et des organismes placés sous sa tutelle dans le domaine du numérique, en facilitant l'émergence d'une filière professionnelle interministérielle dédiée. Il assure également les missions RH de proximité pour la DINUM.

Une mission :

- la mission de l'administratrice générale des données déléguée (AGDD) coordonne et promeut l'action de l'Etat et des organismes placés sous sa tutelle en matière d'inventaire, de gouvernance, de production, de circulation, d'exploitation et d'ouverture des données, et notamment des algorithmes et des codes sources. Elle pilote également le programme « Proactivité ».

Ainsi qu'une cellule :

- la cellule « Cyber » organise l'action de la DINUM en matière de gouvernance de la sécurité des systèmes d'information (SSI), d'anticipation, de détection des événements de sécurité et des réponses à y apporter en lien étroit avec les départements chargés des opérations.

La direction de la DINUM est appuyée par un secrétariat et un cabinet, chargés notamment de la fluidification des échanges, des partenariats institutionnels, industriels, européens et internationaux et de l'appui à l'ensemble des missions et départements de la DINUM.

Dans le but de protéger les produits FranceConnect, les utilisateurs du service et les parties prenantes (agents, partenaires et fournisseurs) contre ces menaces, la DINUM a mis en place une entité dédiée – la Cellule Cyber – à la sécurité du système d'information sous la responsabilité du RSSI et un Système de Management de la Sécurité de l'Information (SMSI) sous la responsabilité du RSMSI.

Le SMSI déployé fait partie intégrante du système de management déjà en place. Ainsi, l'ensemble des membres de la direction soutient l'équipe chargée de sa mise en œuvre en lui donnant les moyens budgétaires et humains pour effectuer sa mission. La direction s'engage également à suivre l'efficacité du SMSI en orientant et en contrôlant sa performance.

La sécurité de l'information est une priorité majeure pour la DINUM convaincue que la protection des données et des systèmes d'information est essentielle pour garantir la confiance des utilisateurs, préserver la réputation de l'organisme et respecter les lois et réglementations en vigueur.

4. PRESENTATION DU SMSI

4.1. ENJEUX

4.1.1 Enjeux Externes

4.1.1.1. FRANCECONNECT

Conformément à l'arrêté du 8 novembre 2018, les téléservices FranceConnect / FranceConnect+ se présentent comme des briques de fédération d'identités qui ont vocation à être reconnues par l'ensemble des administrations et certains acteurs du secteur privé. Elles permettent à un usager français ou européen d'être reconnu par un organisme public en ligne sans disposer préalablement d'un compte d'accès auprès de celui-ci.

Les boutons FranceConnect / FranceConnect+ proposent ainsi à un Usager français ou européen pour FranceConnect+ de s'authentifier via un compte d'accès dans une liste constituée de plusieurs Fournisseurs d'Identité français et européens. Cette liste propose uniquement les Fournisseurs d'Identité présentant un mode d'authentification de niveau de garantie supérieur ou égal à celui demandé par le Fournisseur de Services. Les 3 modes d'authentification de niveaux de garantie eIDAS proposés sont :

- niveau faible : l'objectif est simplement de réduire le risque d'utilisation abusive ou d'altération de l'identité ;
- niveau substantiel : l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité ;
- niveau élevé : l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

Les services FranceConnect / FranceConnect+ ont donc pour ambition de fédérer les identités numériques des usagers et de permettre :

- aux usagers, de bénéficier d'une véritable chaîne de confiance facilitant l'accès aux différents services numériques offerts, de suivre les échanges de données le concernant, de garantir la confidentialité des informations et par conséquent, d'utiliser un même compte d'accès pour effectuer leurs démarches en ligne auprès de diverses entités en s'affranchissant de l'étape d'envoi de pièces justificatives transmises précédemment ;
- aux Fournisseurs de Services, de déléguer la gestion des identités numériques et de l'authentification des usagers à des tiers de confiance Fournisseurs d'Identité.

FranceConnect/FranceConnect+ poursuivent ainsi un double objectif :

- pour les usagers, simplifier et fluidifier les démarches en ligne en améliorant l'expérience utilisateur, ainsi que la sécurisation de l'accès aux démarches en lignes ;
- pour l'Administration et les opérateurs du secteur privé éligibles, mettre en œuvre FranceConnect / FranceConnect+ pour moderniser les services numériques en permettant plus d'interopérabilité entre les systèmes d'information et en accélérant le développement de nouveaux services innovants.

Les boutons FranceConnect / FranceConnect+ ont pour objectif de :

- s'appuyer sur un ou plusieurs des comptes préexistants de l'usager pour être reconnu par tous les opérateurs publics de services en ligne et certains acteurs du secteur privé ;
- profiter de nouveaux services publics numériques sans rupture, centrés sur les besoins des usagers et non sur le découpage organisationnel des structures administratives ;

- assurer la traçabilité et la transparence des données manipulées lors des démarches.

4.1.1.2. REGLEMENT EIDAS

Le Règlement « eIDAS » n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

Il concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne.

Dans le cadre du nœud eIDAS français, seul le premier volet du règlement – portant sur les schémas d'identification électronique nationaux – est concerné.

Le nœud eIDAS français, opéré par la DINUM, est le point de connexion français dans l'architecture de l'interopérabilité d'identification électronique. Il participe au processus d'authentification transfrontalière des usagers français et européens. Pour cela, il a la capacité de reconnaître et de traiter ou d'envoyer des transmissions aux autres nœuds eIDAS européens en permettant à l'infrastructure d'identification électronique nationale de la France de fonctionner en interface avec les infrastructures d'identification électronique nationales d'autres États membres.

Par conséquent, le 1er volet du règlement adresse plusieurs enjeux :

- la levée des obstacles au bon fonctionnement du marché intérieur (problèmes d'interopérabilité transnationale) permettant notamment à l'avenir de s'acquitter de formalités administratives transfrontières de manière plus aisée et rapide, telles que l'inscription d'un étudiant par voie électronique dans une université à l'étranger ou le dépôt en ligne par un contribuable de sa déclaration d'impôts dans un autre Etat membre.
- le renforcement de la confiance dans les transactions électroniques, particulièrement transnationales en instaurant un climat de confiance (cadre juridique, coordination dans le développement et le contrôle des services offerts, transparence quant aux garanties de sécurité et sensibilisation des usagers) afin que les usagers, entreprises et administrations effectuent des transactions par voie électronique et adoptent de nouveaux services en ligne.
- le renforcement de la sécurité juridique lors de l'utilisation de moyen d'identification électronique qu'ils soient qualifiés ou non par la mise en place de règles applicables au sein de l'UE les mêmes pour tous et d'application directe en droit national, les états membres étant tenus de reconnaître les moyens d'identification électroniques notifiés conformément au règlement.

4.1.2 Enjeux Internes

Les enjeux externes présentés précédemment engendrent des enjeux internes pour la DINUM :

- Soutenir l'organisation mise en place chargée d'animer la démarche d'amélioration continue des processus supportant FranceConnect, FranceConnect+ et le nœud eIDAS français :

  Il s'agit pour la DINUM, conformément à l'article 10 paragraphe 1 du règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015, d'apporter la preuve du respect des exigences de la norme ISO/CEI 27001:2022 par certification au travers de la mise en œuvre du SMSI FranceConnect.

La certification ISO/CEI 27001:2022 dépend de la capacité à démontrer le respect des procédures mises en œuvre tout en atteignant l'engagement de service au niveau de la disponibilité de FranceConnect, FranceConnect+ et du nœud eIDAS français, au niveau de l'intégrité des informations échangées, au niveau de la confidentialité des secrets authentifiant les échanges et au niveau de la traçabilité des échanges.

- Impliquer les sous-traitants (actuels et nouveaux à la suite du renouvellement du marché FranceConnect) opérant sur FranceConnect, FranceConnect+ et le Nœud eIDAS français :

  Dans le cadre de marchés publics, la DINUM confie à plusieurs sous-traitants le développement, le déploiement, l'hébergement, l'administration, l'exploitation, la sécurité et le support Usagers & Partenaires de FranceConnect, FranceConnect+ et du Nœud eIDAS français.

- Être l'opérateur du nœud eIDAS français :

  La DINUM, opérateur du Nœud eIDAS français, s'appuie sur la version du nœud eIDAS développée et mise à disposition par l'Union européenne aux 27 États membres.

  En appliquant les spécifications techniques du nœud eIDAS de l'Union européenne, la DINUM garantit l'interopérabilité du nœud eIDAS français avec les autres nœuds européens.

- Maintenir la qualification par l'ANSSI de FranceConnect+ au niveau de garantie substantiel et élevé :

  FranceConnect+, version « renforcée » de FranceConnect, permet de proposer aux usagers des démarches plus sensibles nécessitant des identités de niveaux de garantie « Substantiel » et « Elevé ».

  La DINUM doit donc veiller à maintenir la qualification au niveau de garantie « Elevé » de son service FranceConnect+, afin que son utilisation soit toujours recommandée par l'ANSSI au travers de la liste des produits et services qualifiés de l'ANSSI.

4.1.3 Enjeux Climatiques

4.1.3.1. POUR FRANCECONNECT

Les enjeux internes et externes précédents ne découlent pas des changements climatiques.

Nous avons interrogé les principaux hébergeurs afin de savoir s'ils avaient des enjeux climatiques, et le cas échéant, si des exigences s'appliquaient à FranceConnect.

4.1.3.2. POUR LES HEBERGEURS

4.1.3.2.1. DGFiP – NUBO

4.1.3.2.1.1. Enjeux

Les datacenters utilisés par NUBO sont des datacenters de la DGFIP. Que ce soit côté NUBO et côté DGFIP, il y a une volonté de réduire les impacts environnementaux des datacenters et des matériels. Cela se traduit en général par une réduction de la consommation électrique, grâce à des matériels plus efficients, et aussi via la modernisation des datacenters afin d'optimiser les facteurs PUE, avec des travaux en cours (isolation, réaffectation des locaux, etc.). Ces exigences liées aux changements climatiques rejoignent dans certains cas des enjeux plus économiques, car toutes ces améliorations peuvent aussi se traduire par des économies financières. Une communication plus récente, relayée aussi côté NUBO, vise à appuyer et mettre en avant les orientations dites FinOps, qui à l'origine ne

visaient qu'une réduction des coûts, mais qui aujourd'hui, et particulièrement dans le cas de NUBO en tant qu'hébergeur, se traduisent aussi par une réduction des impacts environnementaux. Cette réduction des impacts environnementaux sont aussi mis en avant côté NUBO avec des incitations, des notions de « Green IT », avec notamment un affichage des estimations des empreintes carbones des ressources consommées sur NUBO. Nous avons aussi la mission EcoGreen, qui s'ajoute à toutes ces exigences que nous nous fixons.

4.1.3.2.1.2. Conséquences pour FranceConnect

Interrogé sur des actions à réaliser côté FranceConnect afin d'aider la DGFIP à atteindre ses objectifs, nous n'avons pas eu de retour à ce jour. Nous réinterrogerons la DGFIP début 2026 sur ce point.

4.1.3.2.2. DGDDI – PA4

4.1.3.2.2.1. Enjeux

Il n'y a pas d'enjeux spécifiquement indiqués, le datacenter d'Osny prend en compte de façon non normative le changement climatique. Cependant le CID [Centre Informatique des Douanes] est en cours de labellisation de la norme ISO 500001 [Systèmes de management de l'énergie] d'ici fin 2025 ou début 2026, cette norme officialisera la prise en compte du changement climatique.

4.1.3.2.2.2. Conséquences pour FranceConnect

Pas de demande spécifiée à ce stade, nous attendons la mise en place de la norme afin de revenir vers la DGDDI pour valider les actions à réaliser.

4.2. OBJECTIFS DU SMSI

L'objectif de cette politique est de définir les principes et les lignes directrices pour la gestion de la sécurité de l'information au sein de la DINUM. Les objectifs stratégiques de mise en œuvre du SMSI sont donc :

- atteindre les objectifs métiers et améliorer la sécurité en interne et des parties prenantes ;
- assurer la continuité des activités métier ;
- assurer le choix de mesures de sécurité adéquates et proportionnées qui protège les actifs et donnent confiance aux parties intéressées ;
- assurer une gestion efficace et efficiente du management de la sécurité de l'information ;
- assurer la mise en place et l'application de la protection du traitement des données des parties prenantes ;
- protéger les données et les systèmes d'information contre les menaces internes et externes ;
- établir des procédures et des mécanismes pour gérer les incidents de sécurité et les violations de la sécurité de l'information.

Ces différents points sont traduits en objectif de sécurité conformément à la PSN DINUM, et sont les suivants :

- **OBJ01** : Maintenir et renforcer la sécurité de l'infrastructure et du système
- **OBJ02** : Soutenir la gouvernance de sécurité mise en place
- **OBJ03** : Améliorer et pérenniser le fonctionnement de l'application

Ils font l'objet de surveillance via des indicateurs définis (cf. §6.3.1).

4.3. DOMAINE D'APPLICATION

4.3.1 Diffusion

La présente politique s'applique à tous les acteurs de l'écosystème FranceConnect, ainsi que ses partenaires et ses fournisseurs. Elle doit être connue de l'ensemble du personnel et acteurs internes du SMSI :

- les RSSI des entités ;
- les services / prestataires en charge des audits ;
- le centre de supervision des incidents de sécurité de la DINUM ;
- les acteurs intervenant au quotidien sur les SI des produits FranceConnect :
  - l'ensemble du personnel FranceConnect ;
  - les partenaires (FI / FS / FD) et fournisseurs (contractuellement ou par le biais de marchés / conventions) dès lors qu'ils stockent, traitent ou utilisent des données issues des SI FranceConnect.

4.3.2 Mise en application

La Politique du SMSI doit être mise en œuvre dès publication pour tous les nouveaux projets sécurité en cours ou à venir FranceConnect.

4.3.3 Dérogations

Les dérogations à cette politique sont, pour une durée limitée, un ensemble de règles qui ne peuvent pas s'appliquer. Ces demandes doivent être formalisées auprès du RSMSI.

4.4. PARTIES INTERESSEES ET LEURS EXIGENCES ENVERS LE SMSI

4.4.1 Liste des parties intéressées

4.4.1.1. SERVICES DU PREMIER MINISTRE (SPM)

La DINUM fait partie des services placés sous l'autorité du Premier ministre. Elle agit donc dans le cadre des grandes orientations fixées par les SPM, notamment en matière de transformation numérique de l'État.

La DINUM a une mission interministérielle, c'est-à-dire qu'elle coordonne les politiques numériques de tous les ministères et agit comme bras armé de l'État en matière de numérique, en coordination avec les SPM, pour s'assurer que les actions sont cohérentes avec les priorités gouvernementales.

4.4.1.2. MINISTRE DE L'ACTION PUBLIQUE, DE LA FONCTION PUBLIQUE ET DE LA SIMPLIFICATION[1]

La DINUM est un service du Premier Ministre, placé sous l'autorité du Ministre de l'Action publique, de la Fonction publique et de la Simplification.

[1] Ministère de rattachement de la DINUM. Ce ministère peut être amené à changer de dénomination.

Le Ministère de l'Action publique, de la Fonction publique et de la Simplification a été créé en janvier 2025 afin d'accélérer l'application des politiques publiques prioritaires dans les territoires, de moderniser les services publics, et de faire évoluer la fonction publique, au service des Français.

4.4.1.3. DIRECTION INTERMINISTERIELLE DU NUMERIQUE (DINUM)

La Direction Interministérielle du Numérique (DINUM), créée par le décret du 25 octobre 2019, a pris la suite de la Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État (DINSIC). Elle a la charge de la transformation numérique de l'État au bénéfice du citoyen comme de l'agent, sous tous ses aspects : modernisation du système d'information de l'État, qualité des services publics numériques, création de services innovants pour les citoyens, outils numériques de travail collaboratif pour les agents.

Dans le cadre du règlement eIDAS, la DINUM assure, en tant qu'« opérateur du nœud eIDAS français », le rôle de point de contact unique en matière d'identification électronique.

Elle est chargée de faire en sorte que les fonctions du nœud eIDAS français en tant que point de connexion soient assurées de manière correcte et fiable.

Pour l'État français, elle a la charge de notifier à l'Union européenne les schémas d'identification des niveaux de garantie substantiel et élevé, les schémas d'identification de niveau de garantie faible ne devant faire l'objet d'aucune notification et être restreint aux échanges nationaux uniquement.

4.4.1.4. AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI)

L'ANSSI, créée par le décret n° 2009-834 du 7 juillet 2009, a la charge de la sécurité des systèmes d'informations de l'État, de conseiller et de soutenir les administrations et les opérateurs d'importance vitale (OIV), ainsi que de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion.

Dans le cadre du règlement eIDAS, l'ANSSI est, en tant qu'« organe de contrôle », en charge de l'évaluation de l'atteinte des niveaux de garantie par les moyens d'identification électronique.

Elle est responsable de l'établissement du cahier des charges pour les exigences applicables à chaque niveau de garantie. Ces niveaux sont accordés en fonction du respect de spécifications, normes et procédures minimales. Trois niveaux de garantie sont prévus par le règlement :

- niveau faible : identifiant/mot de passe. À ce niveau, l'objectif est simplement de réduire le risque d'utilisation abusive ou d'altération d'identité ;
- niveau substantiel : tel que le niveau faible plus un second facteur dynamique. À ce niveau, l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération d'identité ;
- niveau élevé : tel que des certificats qualifiés européens (TS 101 456 ou RGS ***). À ce niveau, l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

Pour la France, seuls les schémas d'identification des niveaux de garantie substantiels et élevés feront l'objet d'une qualification de l'ANSSI, les schémas d'identification de niveau de garantie faible n'ayant pas vocation d'être notifiés à l'Union européenne.

Ces moyens d'identification électronique font l'objet d'une publication dans la liste des produits et services qualifiés de l'ANSSI.

4.4.1.5. LE PROGRAMME INTERMINISTERIEL FRANCE IDENTITE NUMERIQUE

Le Programme Interministériel France Identité Numérique a été mis en place le 5 janvier 2018 par les ministères de l'Intérieur, de la Justice et le secrétaire d'État auprès du Premier Ministre chargé du numérique. Il a la charge de concevoir et de mettre en œuvre des solutions d'identification numérique sécurisées.

L'objectif est de permettre à chaque personne de pouvoir justifier en ligne de son identité de manière simple, sécurisée et garantie par l'État. Cette identification permettra de faciliter certaines démarches administratives sur Internet, mais pourra également être utilisée dans un cadre privé, notamment pour effectuer des achats en ligne ou utiliser des plateformes collaboratives.

L'identité numérique fournie à partir de la Carte Nationale d'Identité électronique (CNIe), est présente sur FranceConnect avec un niveau de garantie « Faible », et est présente sur FranceConnect+ avec un niveau de garantie « Elevé ». La solution opérée se nomme « France Identité ».

« France Identité » est qualifiée aux niveaux « Faible » et « Elevé » jusqu'au 07/02/2026.

4.4.1.6. LA POSTE

La Poste, société anonyme à capitaux publics détenus par l'État français, est à la fois opérateur de services postaux (courrier, colis et express), banque, assurance, opérateur de téléphonie mobile, fournisseur de services numériques et de solutions commerce, commerce en ligne (marketing, logistique) et collecte et vente de données.

Notamment, elle opère le service numérique « L'Identité Numérique La Poste », service d'identité numérique qui permet à un particulier de se doter gratuitement d'une identité numérique vérifiée, de niveau de garantie « substantiel », et ainsi de prouver qui il est.

« L'Identité Numérique La Poste » est qualifiée aux niveaux « Faible » et « Substantiel » jusqu'au 15/01/2026.

4.4.1.7. IDNOW FRANCE

IDnow France, société française créée en 2010, offre un ensemble de solutions sécurisées : de la vérification de documents d'identité, jusqu'à la signature électronique, en passant par la contractualisation digitale.

Elle opère le service numérique « Yris », service d'identité numérique qui permet à un particulier de se doter une fois pour toute d'une identité numérique mobile, de niveau de garantie « faible ».

« Yris » est qualifiée aux niveaux « Faible » et « Substantiel » jusqu'au 14/08/2026

4.4.1.8. COMMISSION EUROPEENNE ET AUTRES ETATS MEMBRES

Conformément à l'article 12, paragraphe 7, du règlement eIDAS, des modalités de procédure ont été définies afin de faciliter la coopération entre les États membres, nécessaire pour assurer l'interopérabilité et la sécurité des schémas d'identification électronique que les États membres entendent notifier ou ont notifiés à la Commission. Elles traitent en particulier de :

- l'échange d'informations, d'expériences et de bonnes pratiques concernant les schémas d'identification électronique et l'examen des évolutions pertinentes dans le secteur de l'identification électronique ;
- l'examen par les pairs des schémas d'identification électronique ;

- la coopération par l'intermédiaire du réseau de coopération.

Les schémas d'identification électronique font l'objet d'une publication au journal officiel de l'Union européenne dans la liste des schémas d'identification électronique notifiés à l'UE.

4.4.2 Attentes des parties prenantes

Les exigences listées ci-après sont :

- ✓ traitées par le SMSI ;
- traitées partiellement par le SMSI, sur le volet sécurité.

4.4.2.1. Services du Premier Ministre (SPM)

L'attestation de conformité de FranceConnect au règlement eIDAS délivrée par l'ANSSI pour les niveaux de garantie « Substantiel » et « Élevé » ainsi que la certification ISO/CEI 27001:2022 du SMSI FranceConnect permettent à la DINUM, en tant que maître d'œuvre de FranceConnect, FranceConnect+ et opérateur du nœud eIDAS français, d'apporter au Premier ministre les preuves :

- ✓ du niveau de sécurité de FranceConnect, FranceConnect+ et du nœud eIDAS français ;
- ✓ du niveau de maturité de la gestion de la SSI dans FranceConnect, FranceConnect+ et nœud eIDAS français ;
- du niveau de conformité aux règlements d'exécution (UE) 2015/1501 et 2015/1502 de la Commission du 8 septembre 2015 ;
- du niveau de conformité aux règlements, directives, lois, décrets et arrêtés applicables à FranceConnect et FranceConnect+ (RGPD, RGS, Loi pour une République numérique, etc.).

4.4.2.2. Ministre de la Transformation et de la Fonction publiques

L'attestation de conformité de FranceConnect au règlement eIDAS délivrée par l'ANSSI pour les niveaux de garantie « Substantiel » et « Élevé » ainsi que la certification ISO/CEI 27001:2022 du SMSI FranceConnect permettent à la DINUM, en tant que maître d'œuvre de FranceConnect, FranceConnect+ et opérateur du nœud eIDAS français, d'apporter à la Ministre de la Transformation et de la Fonction publique les preuves :

- ✓ du niveau de sécurité de FranceConnect, FranceConnect+ et du Nœud eIDAS français ;
- ✓ du niveau de maturité de la gestion de la SSI dans FranceConnect, FranceConnect+ et Nœud eIDAS français ;
- du niveau de conformité aux règlements d'exécution (UE) 2015/1501 et 2015/1502 de la Commission du 8 septembre 2015 ;
- du niveau de conformité aux règlements, directives, lois, décrets et arrêtés applicables à FranceConnect et FranceConnect+ (RGPD, RGS, Loi pour une République numérique, etc.).

4.4.2.3. Direction Interministerielle du Numerique (DINUM)

Du fait de ses missions de performance du Système d'Information unifié de l'État et de transformation numérique de l'action publique concourant à simplifier les relations entre les usagers et les administrations, la DINUM est au cœur de l'interopérabilité d'identification électronique en accomplissant son rôle de point de contact unique en matière d'identification électronique dans le respect des orientations générales arrêtées par l'État et le cadre de la coopération européenne.

L'attestation de conformité de FranceConnect+ au règlement eIDAS délivrée par l'ANSSI pour les niveaux de garantie « Substantiel » et « Élevé » ainsi que la certification ISO/CEI 27001:2022 du SMSI

FranceConnect permettent à la DINUM, en tant que maître d'œuvre de FranceConnect, FranceConnect+ et opérateur du nœud eIDAS français :

- d'instaurer un climat de confiance dans les écosystèmes FranceConnect / FranceConnect+ (partenaires et usagers français et européens) ;
- ✓ d'apporter la preuve du niveau de sécurité ;
- ✓ d'apporter la preuve du niveau de maturité de la gestion de la SSI au sein de FranceConnect / FranceConnect+.

4.4.2.4. AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI)

L'audit global qualifié PASSI de FranceConnect+ sur l'ensemble des portées ainsi que la certification ISO/CEI 27001:2022 du SMSI FranceConnect, permettent à la DINUM, en tant que maître d'œuvre de FranceConnect, FranceConnect+ et opérateur du nœud eIDAS français, d'apporter à l'ANSSI, organe de contrôle du règlement eIDAS les preuves :

- ✓ de conformité de FranceConnect+ et du nœud eIDAS français au règlement eIDAS ;
- ✓ du niveau de sécurité de FranceConnect, FranceConnect+ et du nœud eIDAS français ;
- ✓ du niveau de maturité de la gestion de la SSI dans FranceConnect, FranceConnect+ et nœud eIDAS français ;
- ✓ du respect de l'article 10 paragraphe 1 du règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 ;
- du niveau de conformité aux règlements, directives, lois, décrets et arrêtés applicables à FranceConnect et FranceConnect+ (RGPD, RGS, Loi pour une République numérique, etc.).

4.4.2.5. LE PROGRAMME INTERMINISTERIEL FRANCE IDENTITE NUMERIQUE

L'attestation de conformité de FranceConnect au règlement eIDAS délivrée par l'ANSSI pour les niveaux de garantie « Substantiel » et « Élevé » ainsi que la certification ISO/CEI 27001:2022 du SMSI FranceConnect permettent à la DINUM, en tant que maître d'œuvre de FranceConnect et opérateur du Nœud eIDAS français, d'apporter au programme interministériel France Identité Numérique, maître d'œuvre de l'identité numérique issue de la Carte Nationale d'Identité Electronique (CNIE) les preuves :

- ✓ du niveau de sécurité de FranceConnect, FranceConnect+ et du nœud eIDAS français ;
- ✓ du niveau de maturité de la gestion de la SSI dans FranceConnect, FranceConnect+ et nœud eIDAS français ;
- du niveau de conformité aux règlements d'exécution (UE) 2015/1501 et 2015/1502 de la Commission du 8 septembre 2015 ;
- du niveau de conformité aux règlements, directives, lois, décrets et arrêtés applicables à FranceConnect et FranceConnect+ (RGPD, RGS, Loi pour une République numérique, etc.).

L'ensemble de ces preuves est nécessaire à la publication par l'État français à l'Union européenne du schéma d'identification formé par FranceConnect+ et l'identité numérique issue de la CNIE au niveau de garantie « Substantiel » et « Élevé ».

4.4.2.6. LA POSTE

L'attestation de conformité de FranceConnect au règlement eIDAS délivrée par l'ANSSI pour les niveaux de garantie « Substantiel » et « Élevé » ainsi que la certification ISO/CEI 27001:2022 du SMSI FranceConnect permettent à la DINUM, en tant que maître d'œuvre de FranceConnect et opérateur

du Nœud eIDAS français, d'apporter à la Poste, maître d'œuvre de « L'Identité Numérique La Poste », les preuves :

- ✓ du niveau de sécurité de FranceConnect, FranceConnect+ et du nœud eIDAS français ;
- ✓ du niveau de maturité de la gestion de la SSI dans FranceConnect, FranceConnect+ et nœud eIDAS français ;
- du niveau de conformité aux règlements d'exécution (UE) 2015/1501 et 2015/1502 de la Commission du 8 septembre 2015 ;
- du niveau de conformité aux règlements, directives, lois, décrets et arrêtés applicables à FranceConnect et FranceConnect+ (RGPD, RGS, Loi pour une République numérique, etc.).

L'ensemble de ces preuves est nécessaire à la publication par l'État français à l'Union européenne du schéma d'identification formé par FranceConnect+ et « L'Identité Numérique La Poste » au niveau de garantie « substantiel ». Le schéma français FranceConnect+ et l'identité numérique La Poste a été notifié à la Commission européenne fin 2021 avec des réserves à mettre en œuvre par l'Identité numérique La Poste
https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/France.

4.4.2.7. COMMISSION EUROPEENNE ET AUTRES ETATS MEMBRES

Les exigences suivantes sont traitées par le biais du SMSI :

La publication par l'État français des schémas d'identification formés par FranceConnect+ et les Fournisseurs d'Identité français qualifiés aux niveaux de garantie « substantiel » et « élevé » permet à l'État français d'apporter à la Commission européenne et ses Etats membres les preuves :

- ✓ du niveau de sécurité des schémas d'identification publiés par la France ;
- ✓ du niveau de maturité de la gestion de la SSI au sein des schémas d'identification publiés par la France ;
- de conformité aux règlements d'exécution (UE) 2015/1501 et 2015/1502 de la Commission du 8 septembre 2015.

5. ROLES ET RESPONSABILITES AU SEIN DU SMSI

5.1. LA DIRECTION

Dans le cadre de la présente politique, « la direction » désigne :

- le directeur de la DINUM, qui porte la stratégie globale, répartis les budgets et les postes, et supervise les homologations des services et produits ;
- le responsable de département, qui valide les points clés liés à la gestion des risques et à l'évolution des services;
- le Responsable de la Sécurité des Systèmes d'Information (RSSI), qui est garant de la mise en œuvre opérationnelle des aspects cybersécurité, en coordination avec la cellule cyber.

Ces acteurs travaillent en collaboration via des comités mensuels « cyber » impliquant entre autres le directeur, son adjoint, le responsable de département et le RSSI, pour aborder les sujets de gestion des risques et des évolutions.

5.2. RESPONSABILITES

Les responsabilités pour la sécurité de l'information sont définies comme suit :

- le RSMSI est responsable de la mise en œuvre du SMSI et de la surveillance de cette politique ;
- les agents sont responsables de la sécurité de l'information et doivent prendre des mesures pour la protéger ;
- la direction doit diriger, soutenir, promouvoir et communiquer la Politique de Sécurité du SMSI ;
- la direction a la responsabilité d'assurer que des objectifs et des plans pour le SMSI soient établis et revus annuellement lors de la revue de direction, que les rôles et responsabilités soient définis, qu'un programme de sensibilisation à la sécurité soit communiqué, qu'un audit interne soit mené au moins une fois par année et de fournir les ressources nécessaires au maintien et à l'amélioration du SMSI ;
- la directrice supervise la stratégie globale, les budgets, et les postes, en collaboration avec les responsables de départements. Elle participe également aux homologations des services et produits ;
- le responsable de département valide les décisions clés sur la gestion des risques et répartit les ressources (budget, postes) entre les pôles ;
- la cheffe de pôle est responsable de l'arbitrage des priorités au sein de son pôle, en lien avec les managers ;
- le RSSI et la cellule cyber supervisent les aspects opérationnels liés à la sécurité, en coordination avec le Responsable du Système de Management de la Sécurité de l'Information (RSMSI) ;
- chaque chef de département a la responsabilité d'assurer que les personnes qui travaillent sous son contrôle protègent l'information conformément aux politiques de la DINUM ;
- le personnel de la DINUM (direction, ensemble du personnel et contractants) doit être sensibilisé aux risques pesant sur la sécurité de l'information, de leurs responsabilités, et de la

nécessité de respecter les politiques ainsi définies pour assurer une protection adéquate de l'information dans le cadre de leur activité normale.

6. FONCTIONNEMENT DU SMSI

6.1. REVUE DES OBJECTIFS DU SMSI

Les objectifs du SMSI sont réévalués lors de la Revue de Direction annuelle. L'analyse des données, processus, tableaux de bord et indicateurs permet d'identifier les axes d'amélioration du SMSI. Les résultats de l'appréciation et du traitement des risques sont également présentés à la Direction pour ajuster les objectifs du cycle suivant.

Les nouveaux objectifs sont ensuite transmis aux instances de pilotage du SMSI pour faciliter la mise en œuvre des actions d'amélioration, lesquelles sont planifiées et actualisées si besoin (responsables, délais).

6.2. DOCUMENTATION DU SMSI

Au sein d'un SMSI (Système de Management de la Sécurité de l'Information), la documentation joue un rôle essentiel pour démontrer la conformité à la norme ISO/IEC 27001:2022.

6.2.1 Type de document

Afin d'assurer une gestion efficace de la sécurité de l'information, les documents sont classés selon différents types :

1. Politique

   Document qui définit les objectifs de la politique de sécurité de l'information et le caractère obligatoire des instructions dérivées. Cela inclut :

   - la Politique du SMSI de FranceConnect (c'est-à-dire ce document) : document directeur qui définit l'engagement de la direction envers la sécurité de l'information.
   - la Politique de Sécurité du SMSI de FranceConnect ;
   - la Politique de Sécurité du Numérique de la DINUM (PSN DINUM) ;

2. Plan

   Document structuré qui définit les actions à mener, les ressources à mobiliser, les responsabilités, les délais, et les objectifs à atteindre pour répondre à un besoin spécifique lié à la sécurité de l'information. C'est un document de gestion opérationnel ou stratégique, conçu pour organiser et anticiper les activités nécessaires à la mise en œuvre, au maintien, à la surveillance ou à l'amélioration continue du SMSI. Par exemple :

   - Plan de traitement des risques ;
   - Plan de continuité d'activité (PCA) ;
   - Plan de reprise d'activité (PRA) ;
   - Plan de classification ;
   - Plan d'actions.

3. Procédure

   Document qui décrit les processus, les responsabilités des acteurs et comment les exigences de sécurité sont mises en œuvre. Par exemple :

- Procédure de gestion des incidents de sécurité ;
- Procédure de contrôle d'accès ;
- Procédure de sauvegarde ;
- Procédure de gestion des changements ;
- Procédure de gestion des non-conformités.

4. Enregistrements / Preuves

Tous autres documents / éléments qui peuvent servir de preuve de la bonne exécution de la gestion de la sécurité de l'information, tels que :

- registre des interventions des équipes FC sur le DC d'Osny ;
- journal des événements ;
- rapports d'audit ;
- journal des incidents ;
- rapports de sauvegarde / de restauration ;
- comptes-rendus de revues de direction ;
- preuves de formation / de sensibilisation du personnel ;
- etc.

5. Documents de référence / Annexes

Document externe ou interne utilisé comme base ou source d'information pour élaborer, appliquer ou justifier un élément du système. Il peut s'agir de normes, lois, règlements, politiques internes ou guides techniques. Par exemple :

- Externe
  - ISO/IEC 27001 : Norme principale pour la mise en œuvre d'un SMSI ;
  - ISO/IEC 27002 : Guide de bonnes pratiques pour les contrôles de sécurité ;
  - RGPD (Règlement Général sur la Protection des Données) : Obligations légales en matière de données personnelles ;
  - Méthode EBIOS Risk Manager ;
- Interne :
  - déclaration d'applicabilité : document obligatoire qui liste les contrôles de l'annexe A de l'ISO 27001 et justifie leur inclusion ou exclusion ;
  - la Méthodologie d'Appréciation des Risques ;
  - fiches de poste ;
  - charte utilisateur / administrateur.

6.2.2 Rôles

Chaque document constituant le corpus documentaire du SMSI, doit avoir un rédacteur identifié ainsi qu'un contrôleur et/ou un approbateur.

Type de document	Rédacteur	Contrôleur	Approbateur
Politique	RSMSI	Responsable Pôle Identité Numérique (1)	Chef de Département
Plan	Responsable du plan	RSMSI	RSSI
Procédure	Responsable de la procédure	RSMSI	Responsable d'équipe / autre responsable (2)
Enregistrement	Propriétaire de la donnée	Optionnel (3) / RSMSI	Optionnel (3) / RSMSI
Document de référence interne	Responsable / porteur du document	Optionnel (3) / RSMSI	Optionnel (3) / RSMSI / porteur du document

(1) Le RSSI ou tout autre responsable désigné par le RSMSI peut être amené à relire et amender la politique (notifié dans l'historique du document).

(2) Si le responsable de l'équipe (support, développement, etc.) est aussi le rédacteur de la procédure, le RSMSI pourra demander à un autre responsable, ayant des connaissances ou étant partie prenante de la procédure (par exemple le RSSI) de l'approuver. A titre exceptionnel et dérogatoire, validée par le RSMSI, le rédacteur peut être approbateur de la procédure.

(3) Certains documents, de par leur nature, ne nécessitent pas spécifiquement un contrôleur ou un approbateur. Le RSMSI jugera au cas par cas.

6.3. EVALUATION DE LA PERFORMANCE

6.3.1 Surveillance et analyse

Afin de s'assurer de l'atteinte des objectifs, tant sécurité que métier, différents indicateurs ont été définis. Ces indicateurs sont suivis individuellement et périodiquement par le Responsable du SMSI. Les fichiers de suivi des indicateurs sont enregistrés dans le référentiel documentaire.

6.3.1.1. INDICATEURS STRATEGIQUES

- ST01-UTILISATEURS : nombre d'utilisateurs actifs mensuels de FC et FC+ sur les 3 dernières années ;
- ST02-COMITOLOGIE : nombre de tenue de revue de direction et de comité de pilotage SSI (COPIL-SSI) par an ;
- ST03-REVUES_2700X : revues des principaux documents 27001 et 27002 ;
- ST04-RH : évolution du personnel depuis 2017 (arrivées/départs) + répartition par équipe ;
- ST05-PARTENAIRES-NB : évolution du nombre de FI/FS/FD actifs par niveau et par privé/public pour FC et FC+
- ST06-PARTENAIRES-CO : évolution du nombre de connexion aux FI/FS/FD actifs par niveau et par privé/public pour FC et FC+ ;
- ST07-SSSI : suivi de la sensibilisation du personnel ;
- ST08-PA : traitement des risques ;
- ST09-MATURITE : évaluation de la maturité du SMSI ;
- ST10-NB_RESSOURCES-IMP : nombre de ressources impliquées dans les rôles clés du SMSI ;

- ST11-CHARGE : charge de travail dédiée au SMSI ;
- ST12-NB_RESSOURCES-EMP : nombre de ressources employées au fonctionnement du SMSI.

6.3.1.2. *Indicateurs Operationnels*

- OP01-DISPO : disponibilité du téléservice et des composants FC/FC+ (par année civile et mois) ;
- OP02-INCIDENTS : suivi des fraudes (usurpation) / phishing / évènements de sécurité ;
- OP03-CONTROLES_INTERNES : suivi de l'application du processus du contrôle interne (respect des contrôles à effectuer selon les fréquences et actions indiquées) ;
- OP04-BUGBOUNTY : suivi du nombre de rapports validés sur le bug-bounty de FC/FC+/eIDAS ;
- OP05-DELAI : délai de traitement des incidents par criticité : vulnérabilités sur les composants SAST et dépendances, écarts/vulnérabilités détectés lors des audits.

6.3.2 Audits du SMSI

Les audits du SMSI sont réalisés sous la responsabilité de l'équipe de sécurité opérationnelle. Ils sont menés par ou pour le compte de la DINUM conformément au planning prédéterminé.

Les objectifs du programme d'audit, sa planification, la réalisation et la diffusion des rapports d'audit sont détaillés dans le suivi des audits du SI et du SMSI.

6.3.3 Instances de gouvernance

6.3.3.1. *Comite de direction SSI (CODIR SSI)*

Le CODIR SSI présidé par la directrice a lieu à une fréquence minimale de 6 fois par an et a pour objectif la présentation, le suivi et la mise à jour des actions SSI de la DINUM. Le comité permet également d'assurer un suivi des budgets. Celui-ci est composé des acteurs impliqués dans la SSI (RSSI, chefs de pôle) ainsi que le RSMSI chargé de remonter les points relatifs au SMSI.

6.3.3.2. *Comite de pilotage FranceConnect (COPIL FC)*[2]

Un comité de pilotage FranceConnect est organisé de manière hebdomadaire afin d'orienter la prise de décision pour les intervenants sur le périmètre FranceConnect : responsable du pôle, directeur technique, directeur produit, responsable innovation, responsable exploitation, responsable partenariat, responsable support, ainsi que le RSMSI. Ce COPIL FC est l'occasion pour le RSMSI :

- d'identifier d'éventuels changements dans le SI FranceConnect pouvant impacter le SMSI ;
- de rappeler les prochaines échéances ;
- de valider avec la responsable FranceConnect les ressources mises à disposition pour le SMSI ;
- de s'assurer de la bonne mise en œuvre du plan d'action du SMSI.

6.3.3.3. *Reunions eIDAS*

Dans le cadre du règlement eIDAS, les correspondants eIDAS de la DINUM participent :

- aux revues par les pairs des schémas d'identification publiés par les États membres pour le Règlement eIDAS ;
- aux réunions techniques relatives au Règlement eIDAS avec les États membres.

[2] Un suivi opérationnel est réalisé par l'équipe SMSI. Voir la procédure de « Gestion des Actions et des Non-Conformités ».

6.3.3.4. REVUE DE DIRECTION

Les revues de direction du SMSI ont lieu annuellement. Une revue intermédiaire est possible si des décisions urgentes sont nécessaires.

Ces réunions, présidées par la direction, visent à valider l'adéquation et l'efficacité du SMSI selon la directive et les objectifs, et à définir ses orientations futures.

Les résultats des revues de direction sont consignés dans un compte-rendu détaillant les décisions et actions sur les sujets abordés.

6.4. AMELIORATION CONTINUE ET GESTION DES NON-CONFORMITES

La DINUM promeut une culture d'amélioration continue à tous les niveaux. Les formations et sensibilisations permettent au personnel FranceConnect d'identifier les conditions nécessaires pour respecter les exigences de sécurité de l'information et à réagir efficacement aux situations impactant cette sécurité.

De même, des actions correctives sont mises en œuvre pour éliminer les causes de non-conformités, éviter leurs récidives, et prévenir l'apparition de non-conformités similaires. Ce traitement fait partie intégrante de l'évaluation des risques et de l'amélioration continue.

Le traitement des actions correctives est détaillé dans la procédure « Gestion des actions et des non-conformités ».

L'ensemble des actions correctives et préventives est consigné dans le plan d'actions du SMSI FranceConnect (GitLab).

7. EXIGENCES REGLEMENTAIRES ET LEGALES

La politique de sécurité numérique de FranceConnect est établie en conformité avec les lois et règlements en vigueur, notamment :

- Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique ;
- Arrêté du 8 novembre 2018 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication (DINSIC) d'un téléservice dénommé « FranceConnect » ;
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée, version consolidée du 6 août 2018 ;
- Référentiel Général de Sécurité – Version 2.0 du 13 juin 2014 ;
- Instruction interministérielle n°901 SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'information sensibles ;
- Politique de Sécurité des Systèmes d'Information de l'État – Version 1.0 du 17 juillet 2014.
- Le règlement européen (UE) n° 910/2014 (eIDAS), adopté par le Parlement européen et le Conseil de l'Union européenne le 23 juillet 2014, établit un cadre juridique pour l'identification électronique et les services de confiance (signature électronique, horodatage, cachet électronique, etc.) au sein du marché intérieur de l'Union européenne

FIN DU DOCUMENT