PREMIER MINISTRE

Liberté
Égalité
Fraternité

Direction interministérielle du numérique

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

Version 1.2

Propriétés du document

	Identité	Date
Rédacteur	Laurent BARRAT	04/09/2024
Contrôleur	Linda DEBERNARDI	05/11/2024
Approbateur	Florian DELEZENNE	13/12/2024

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

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 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. POLITIQUE DE SECURITE DE L'INFORMATION

1.1. CONTEXTE

Simplifier l'accès aux démarches administratives en ligne de tous les Français, c'est la promesse de FranceConnect créé en 2016 et opéré par la Direction interministérielle du numérique (DINUM) intervenant sous l'égide du ministère de la Transformation et de la Fonction publiques. Aujourd'hui, 1400 services sont accessibles via FranceConnect, et 44 millions d'usagers font confiance au service.

L'actualité témoigne des risques liés à l'évolution des usages numériques : fuite d'informations, perte ou réduction d'activité, atteinte à l'image de marque, exploitation excessive de données personnelles.

1.2. POLITIQUE DE SECURITE DE L'INFORMATION

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.

1.3. ENJEUX

1.3.1 Enjeux Externes

1.3.1.1. 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 : au moins un facteur d'authentification de type identifiant/mot de passe (uniquement pour des FI français) ;

- niveau substantiel : au moins deux facteurs d'authentification de différentes catégories, le respect des exigences du niveau faible ainsi qu'un facteur dynamique, le moyen d'authentification est qualifié de niveau élémentaire RGS (FI français et européens notifiés pour le niveau « substantiel ») ;
- niveau élevé : au moins deux facteurs d'authentification de différentes catégories, le respect des exigences du niveau substantiel ainsi qu'un facteur de type biométrique ou photographique, le moyen d'authentification est qualifié de niveau renforcé RGS.

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 poursuit ainsi un double objectif :

- pour les usagers, simplifier et fluidifier les démarches en ligne en améliorant l'expérience utilisateur ;
- 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.

1.3.1.2. 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.

1.3.2 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 des marchés « Réalisation de services publics numériques en mode produit coordonnés par le programme interministériel Beta.gouv » et « Prestations d'accompagnement au support et à la sécurité du produit FranceConnect et de ses produits dérivés », 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.

1.3.3 Enjeux Climatiques

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

1.4. 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 de la 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.

1.5. Principes de la Politique du SMSI

Pour l'atteinte de ces objectifs, 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 (cf. §4 Exigences Réglementaires et Légales) ;
- la politique a été approuvée par la direction et est l'objet d'un réexamen annuel.

1.6. DOMAINE D'APPLICATION

1.6.1 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.

1.6.2 Mise en application

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

1.6.3 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.

1.7. RESPONSABILITES

1.7.1 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 le directeur, son adjoint, le responsable de département et le RSSI, pour aborder les sujets de gestion des risques et des évolutions.

1.7.2 Responsabilités

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 ;
- le directeur supervise la stratégie globale, les budgets, et les postes, en collaboration avec les responsables de départements. Il supervise également les 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 ;
- le chef 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) doivent être sensibilisés 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.

1.8. Revision et Mise a jour

La présente Politique de Sécurité 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 les changements juridiques.

1.9. Engagement de la Direction

L'application opérationnelle de cette politique de sécurité 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 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.

Pour la direction :

Stéphanie Schaer
Directrice interministérielle du numérique

Date et signature : le 13 janvier 2025

2. INDICATEURS SUIVIS

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.

2.1. INDICATEURS STRATEGIQUES

- ST01-UTILISATEURS : nombre d'utilisateurs actifs mensuels de FC et FC+ sur les 3 dernières années ;
- ST02-COMITOLOGIE : nombre de tenue du Comité de Direction ;
- 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.

2.2. 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.

3. STRUCTURE DE LA POLITIQUE DE SECURITE DU SMSI

Les documents du SMSI sont classés en cinq niveaux :

1. Politiques de sécurité de l'information : documents qui définissent les objectifs de la politique de sécurité de l'information et le caractère obligatoire des instructions dérivées. Cela inclut la politique du SMSI (c'est-à-dire ce document) et les politiques spécifiques au domaine (politique organisationnelle, politique de gestion des risques, politique de classification des actifs, etc.) ;
2. Plans : documents qui contiennent des indications tactiques sur quand et comment les objectifs seront atteints dans chaque domaine (domaine d'applicabilité, déclaration d'applicabilité de chaque entité, plans de traitement des risques, plans d'action pour atteindre les objectifs, liste des exceptions, résultats d'évaluation et traitement des risques, etc.) ;
3. Procédures : documents qui décrivent les processus et les responsabilités des acteurs (processus de classification des biens, processus de gestion des données de sortie, processus d'installation du système informatique, etc.) ;
4. Standards : documents qui contiennent les instructions et les règles de sécurité (instructions de gestion, codes de conduite, règles de sécurité applicables aux informations classifiées, liste des outils cryptographiques acceptés, etc.) ;
5. Enregistrements : tous autres éléments qui peuvent servir de preuve de la bonne exécution de la gestion de la sécurité de l'information (registre des visiteurs, journal des événements, etc.).

4. 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.

FIN DU DOCUMENT