Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

Convention de partenariat entre Syndicat Intercommunal des Technologies de l'Information pour les Villes (SITIV) et la Direction générale des Finances publiques en vue de l'exposition de documents de rémunération sur le portail ENSAP

Entre :

Syndicat Intercommunal des Technologies de l'Information pour les Villes, représenté par Monsieur Vangheluwe Stéphane, Directeur Général des Services, 50 bd Ambroise Croizat 69200 Vénissieux ci-après dénommé « SITIV », d'une part,

et :

La Direction générale des Finances publiques au sein du ministère de l'Économie, des Finances et de l'Industrie, représentée par Monsieur David KARLE, sous-directeur, responsable du département du programme de modernisation au service des Retraites de l'État, 10 boulevard Gaston Doumergue 44 964 Nantes Cedex 9, ci-après dénommée « la DGFiP », d'autre part,

ci-après collectivement dénommées « les parties ».

il est convenu ce qui suit :

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

Préambule

La Direction générale des Finances publiques met en œuvre le traitement dénommé ENSAP (Espace numérique sécurisé des agents publics) qui a notamment pour finalité de mettre à la disposition des agents publics un espace d'archivage de documents relatifs à la paye. Ce traitement est autorisé par le décret n°2022-1446 du 21 novembre 2022, pris pour l'application du décret n°2016-1073 du 3 août 2016 relatif à la mise à disposition et à la conservation sur support électronique des bulletins de paye et de solde des agents publics, modifié par décret n°2021-1752 du 21 décembre 2021 relatif aux modalités d'utilisation par certaines personnes morales de droit public de l'espace numérique sécurisé des agents publics et modifiant la durée de conservation des données au sein de ce traitement.

Ce traitement a été soumis à avis préalable de la CNIL rendu dans sa délibération n° 2022-109 du 10 novembre 2022.

L'Espace Numérique Sécurisé de l'Agent Public (ENSAP), offre de service internet sécurisée développée et administrée par la DGFiP, améliore et simplifie l'accès des agents à leurs documents de rémunération (bulletins de paye ou de salaire, décomptes de rappel, attestations fiscales), en les mettant à leur disposition sous forme dématérialisée dans un espace personnel performant et ergonomique, accessible par internet 7 jours sur 7.

L'agent dispose de deux modalités distinctes d'accès à l'espace numérique sécurisé : par un dispositif d'authentification (DAC/LDAP) spécifique par un couple login (NIR) - mot de passe, ainsi que par le service FranceConnect qui est un mécanisme de fourniture d'identité et d'authentification numérique pour les usagers. FranceConnect permet également le suivi par l'usager des échanges de données le concernant et garantit la confidentialité des informations.

Article 1. Objet de la convention

Le présent document a pour objet de définir les conditions et modalités de collaboration entre la DGFiP et SITIV en vue d'exposer dans l'ENSAP les documents de paye des agents rémunérés par ce dernier.

La présente convention vaut convention de mise à disposition de l'ENSAP auprès des agents de SITIV au sens de l'article 7 du décret n° 2016-1073 du 3 août 2016 modifié relatif à la mise à disposition et à la conservation sur support électronique des bulletins de paye et de solde des agents publics.

Article 2. Suivi des questions de sécurité

- L'AQSSI (Autorité Qualifiée pour la Sécurité des Systèmes d'Information) de Ia DGFIP est le Directeur général des Finances publiques. Le RSSI (Responsable de la Sécurité des Systèmes d'Information) représente l'AQSSI de la DGFiP. En particulier, la sécurité de l'ENSAP fait partie de son périmètre de responsabilité. Ces fonctions sont exercées par le responsable de la division DMOCSS et par son adjoint, par délégation.

- Pour SITIV, l'AQSSI est le Directeur Général des Services de l'intéressé . Le RSSI (Responsable de la Sécurité des Systèmes d'Information) représente l'AQSSI sur les aspects opérationnels et est l'interlocuteur unique de la DGFiP pour ce qui concerne les dispositions de sécurité relevant de la présente convention. Le périmètre de ses responsabilités comprend :

le contrôle du respect des règles d'emploi et de sécurité de l'ENSAP définies par la DGFIP,

le transfert des données vers l'ENSAP.

Article 3. Rôle et engagements de la DGFIP

La DGFiP agit en tant que fournisseur de service, et, à ce titre, doit assurer la sécurité et la confidentialité des informations personnelles lorsqu'elles transitent et sont stockées dans son système d'informations et ce dès leur prise en charge.

La DGFiP met en œuvre et opère les échanges des données et des flux conformément aux dispositions réglementaires et légales en vigueur.

La DGFiP est responsable des données reçues, traitées, stockées, diffusées par l'ENSAP, y compris les données techniques afférentes. A ce titre, elle garantit la bonne utilisation de l'ENSAP par toutes les parties prenantes au système et détermine les conditions d'utilisation, les règles d'emploi et de sécurité du système et veille à leur respect.

La DGFiP réalise les développements informatiques nécessaires au fonctionnement des services. Elle assure l'hébergement et l'exploitation des applicatifs et de toute l'infrastructure nécessaire au fonctionnement des back et front offices.

La DGFiP s'engage sur une simple mise à disposition des documents transmis par le fournisseur de données, à l'exclusion de toute autre utilisation des données et documents transmis par celui-ci. À réception des flux, la DGFIP assure la restitution d'un accusé de traitement par ATLAS et d'un fichier retour fonctionnel de collecte des données par l'ENSAP.

L'offre générale de mise à disposition des documents est adossée à une offre d'archivage des documents PDF dans le silo ATLAS, jusqu'aux 75 ans de l'usager ou jusqu'à deux ans après son décès.

Il est rappelé que, conformément à l'article 1 du décret n°2022-1446 du 21 novembre 2022 précité, la mise en œuvre du traitement ENSAP par la DGFiP est nécessaire au respect d'une obligation légale.

La mise à disposition des bulletins de paie des agents ne nécessite aucune option particulière de ces derniers (*référence de la décision du conseil de surveillance ou de l'organe délibérant de la collectivité ou de l'établissement public* de *SITIV* du *date* portant application du décret n° 2016-1073 du 3 août 2016 modifié relatif à la mise en place et à la conservation sur support électronique des bulletins de paye et de solde des agents publics).

La DGFiP présente à l'usager tous les éléments d'informations nécessaires pour l'utilisation du Portail. Le Portail est accessible aux agents de SITIV à un niveau de disponibilité dit « fort » au sens de la DGFIP (cf. annexe 1). La durée de conservation des données d'identification et des logs ENSAP est de 12 mois à compter de leur enregistrement.

La DGFiP ne peut intervenir sur les données de SITIV sans son autorisation explicite. Elle s'engage à fournir à SITIV toutes les informations utiles et nécessaires en cas d'événement de sécurité de nature à affecter le système d'information dont elle est responsable.

Sur la sollicitation de SITIV, la DGFiP s'engage à coopérer avec lui/elle, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à permettre l'exercice, par les personnes concernées, de leurs droits d'accès et de rectification prévus par la réglementation.

Article 4. Rôle et engagements du SITIV

Dans le cadre du Portail ENSAP, SITIV est fournisseur de données. Il s'engage à transmettre les données et documents personnels nécessaires à l'application de la présente convention et à ne pas communiquer de données non utiles à celle-ci.

Il incombe à SITIV de supprimer de ses envois vers la DGFiP les informations qu'il jugerait très sensibles ou incompatibles avec le niveau de protection mis en œuvre par ce dernier. Notamment, les informations relevant d'une diffusion restreinte ne doivent pas être transmises à la DGFIP.

Il incombera à SITIV d'informer ses personnels de toute modification qui serait introduite sur les documents ou données transmises.

Le SITIV s'engage à transmettre les métadonnées et bulletins de paie au format PDF/A après chiffrement, conformément au format d'échange technique décrit dans la documentation fournie lors de l'ouverture du projet (DGFiP : SSI et SRE ; le SITIV).

[Les flux seront transmis via le réseau interministériel de l'Etat (RIE) et devront être chiffrés.]

La DGFiP refusera la réception des flux non conformes aux spécifications techniques.

Le SITIV s'engage à fournir à la DGFiP toute information utile et nécessaire en cas d'événement de sécurité de nature à affecter le système d'information dont elle est responsable.

Article 5. Obligations relevant du règlement européen n° 2016/679 du 27 avril 2016, de la loi n° 78-17 du 6 janvier 1978 modifiée par la loi 2018-493 du 20 juin 2018 et du décret n°2010-112 du 2 février 2010

La DGFiP, en tant que co-traitant, et le SITIV, en tant que fournisseur de données, s'engagent à respecter les obligations inhérentes aux échanges induits par l'ENSAP, notamment celles, détaillées ci-dessous, relevant de la loi n° 78-17 du 6 janvier 1978 modifiée par la loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles, celles du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et celles relevant de l'ordonnance n°2005-1516 du 8 décembre 2005 et du décret n°2010-112 du 2 février 2010 relative au Référentiel Général de Sécurité.

La confidentialité et la disponibilité des données à caractère personnel durant toute l'exécution de la présente convention et après son expiration.

La prise de toutes mesures nécessaires telles que définies aux articles 6 et 7 de la présente convention pour préserver la sécurité et la confidentialité des données et empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

- Effectuer les formalités auxquelles la DGFIP et le SITIV sont astreint(e)s en tant que responsables de traitement de leur système d'information respectif. Les informations sur la réalisation de celles-ci doivent être communiquées à la partie qui en fait la demande.

- Répondre aux usagers concernant leurs demandes de droit d'accès et de rectification. Ces droits s'exercent pour les données concernant la paye auprès de le SITIV et pour les données d'authentification et de connexion au portail ENSAP auprès de la DGFIP.

Article 6. Confidentialité des données et secret professionnel

Les parties sont tenues, ainsi que l'ensemble de leur personnel, au secret professionnel, à l'obligation de discrétion et à l'obligation de confidentialité durant toute l'exécution de la présente convention et après son expiration.

Les parties conviennent que les données transmises à la DGFiP ne doivent en aucun cas être divulguées ou retransmises à des personnes physiques ou morales non autorisées.

Les parties s'interdisent toute communication d'informations écrite ou verbale sur ces sujets ou toute remise de documents à des tiers sans l'accord préalable et écrit de l'autre partie.

Les parties s'engagent à respecter de façon absolue lesdites règles et obligations, et à les faire respecter par les utilisateurs qu'ils auront autorisés à accéder aux services.

Si, pour l'exécution de la présente convention, les parties ont recours à des prestataires de services traitant des données à caractère personnel pour le compte du responsable du traitement, ceux-ci doivent être considérés comme des sous-traitants au sens de la loi 78-17 du 6 janvier 1978 modifiée et présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité. Cette exigence ne décharge pas le responsable de traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement doit comporter toutes les indications permettant le respect des dispositions de l'article 28 du règlement européen sur la protection des données n° 2016/679.

<u>Contrôle sur les personnels en charge d'intervenir et de maintenir les applications</u>

Les parties s'engagent à faire souscrire à ces prestataires de services, en plus des engagements contenus dans le présent article, les engagements suivants :

- ils ne doivent pas utiliser les documents et supports d'information confiés par l'une des parties à des fins autres que celles spécifiées à la convention,
- ils ne doivent conserver aucune copie des documents et supports d'information confiés par l'une des parties après l'exécution des prestations,
- ils ne doivent pas communiquer ces documents et informations à d'autres personnes que celles qui ont qualité pour en connaître,
- ils doivent prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers en cours d'exécution de la présente convention,
- ils doivent prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la convention,

- ils doivent reconstituer les documents et les fichiers qui leur sont confiés et qui viendraient à être perdus ou inutilisables par leurs fautes.

Dans le cas où les prestataires de services sous-traiteraient l'exécution des prestations à un tiers, ce dernier serait soumis aux mêmes obligations.

Article 7. Sécurité

Les parties s'engagent à prendre toutes les mesures utiles pour assurer, lors de l'exécution de la convention, la protection des informations ou supports protégés qui peuvent être détenus ou échangés par les parties.

La mise en œuvre de certificats avec authentification mutuelle est obligatoire pour tout échange, de même que l'implémentation rigoureuse des règles d'appels telles que définies dans l'annexe 4 en conformité avec le RGS. Les deux parties s'engagent à se communiquer toute information utile et nécessaire en cas d'événement de sécurité.

La DGFiP est responsable de l'homologation de sécurité du Portail ENSAP et de son maintien en condition de sécurité.

Sur demande, chacune des parties communiquera la décision d'homologation de son système d'information visé par la présente convention de partenariat.

Le site ensap.gouv.fr est un site du Ministère en charge de l'Économie, des Finances et de l'Industrie, dont les modalités d'utilisation sont encadrées par le décret n°2022-1446 du 21 novembre 2022 précité.

Article 8 : Protection des données à caractère personnel et notification des violations de données personnelles

SITIV et la DGFIP, sont co-responsables du traitement des données de l'ENSAP pour les agents rémunérés par SITIV.

SITIV s'engage à informer ses agents de la mise en œuvre du traitement ENSAP, ainsi que des conditions dans lesquelles ils peuvent demander l'accès, la rectification de leurs données personnelles. SITIV informe ses agents des coordonnées de son DPO.

8-1. Gestion des incidents de sécurité, notamment les violations de données à caractère personnel

Les Parties gèrent les incidents de sécurité, y compris les violations de données à caractère personnel, conformément à leurs procédures internes et à la législation applicable.

Les Parties se prêtent en particulier mutuellement une assistance rapide et efficace, le cas échéant, pour faciliter l'identification et la gestion de tous les incidents de sécurité, notamment les violations de données à caractère personnel, liées à au traitement conjoint.

Les Parties se notifient mutuellement:

a) tout risque potentiel ou réel pour la disponibilité, la confidentialité, et / ou l'intégrité des données à caractère personnel traitées conjointement ;

b) tout incident de sécurité lié au traitement conjoint ;

c) toute violation de données à caractère personnel (c'est-à-dire toute violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la

divulgation non autorisée de données à caractère personnel ou l'accès non autorisé aux données traitées conjointement) ;

d) toute faille dans les garanties techniques ou organisationnelles de l'opération de traitement conjointe.

La notification de violation des données à caractère personnel aux autres responsables conjoints contient au-moins :

- la description de la nature de la violation des données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- l'évaluation du risque pour les droits et libertés des personnes physiques ;
- la description des mesures prises pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Chaque Partie est responsable de tous les incidents de sécurité, y compris les violations de données à caractère personnel, qui se produisent en conséquence d'une violation des obligations de cette partie en vertu de cet accord et du Règlement (UE) 2016/679.

Les Parties documentent les incidents de sécurité (y compris les violations de données à caractère personnel) et se les notifient mutuellement dans les meilleurs délais et au plus tard 72 heures après avoir pris connaissance d'un incident de sécurité (y compris une violation de données à caractère personnel).

La Partie, responsable d'une violation de données à caractère personnel, documente cette violation de données à caractère personnel et la notifie à la Commission nationale de l'informatique et des libertés. Cette notification doit être effectuée dans les meilleurs délais et, si possible, 72 heures au plus tard après avoir pris connaissance de la violation de données à caractère personnel, à moins que la violation de données ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. La Partie responsable doit informer les autres parties de cette notification.

La Partie, responsable de la violation de données à caractère personnel, communique cette violation de données à caractère personnel aux personnes concernées si la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. La Partie responsable doit informer les autres Parties de cette communication.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données du responsable conjoint concerné ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises pour remédier à la violation y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

8-2. Coordonnées des RSSI et DPD

RSSI SITIV :

Hibert Sylvain
RSSI

Ou par mail : shibert@sitiv.fr

RSSI DGFiP : Monsieur le Directeur général des Finances publiques
Monsieur le responsable de la division DMOCSS
bureau.si3-dmocss@dgfip.finances.gouv.fr

DPD SITIV :

Hibert Sylvain
DPD

Ou par mail : shibert@sitiv.fr

DPD DGFiP :

Monsieur le délégué à la protection des données du ministère économique et financier
Délégation aux Systèmes d'Information
139, rue de Bercy Télédoc 322. 75572 PARIS CEDEX 12
le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr

Article 9 : Circuit d'assistance

Le circuit d'assistance aux agents est décrit dans le Guide du gestionnaire de la paie remis à le SITIV. Il emporte toutes les conséquences liées à des défaillances portées par les flux de documents de paie : inscription à l'ENSAP, accès au service d'exposition des documents de paie.

Pour tout autre question des internautes sur le portail, l'internaute dispose d'un assistant virtuel et de FAQ.

Article 10 : Rétrocession des documents transmis par l'employeur

Le silo de stockage ATLAS, de la DGFiP, prévoit la possibilité, pour l'émetteur de documents PDF conservés dans ce silo, de rétrocéder ces documents, sur la base d'une demande expressément formulée à l'adresse électronique suivante : bureau.bsi2-atlas@dgfip.finances.gouv.fr. Cette rétrocession entraînera : la restitution à l'émetteur originel de l'ensemble des documents demandés, ainsi que la purge de ces mêmes documents de la plateforme ATLAS. ATLAS informera l'ENSAP des documents dont il conviendra de purger les métadonnées correspondantes.

Article 11 : Évolutions

La DGFIP s'engage à prévenir le SITIV de tout projet d'évolution des flux et des spécifications associées avec un délai de prévenance trois mois. Le nouveau format de flux sera mis en production par l'ENSAP en tenant compte du délai de réalisation des évolutions par le SITIV pour son propre flux de collecte.

Article 12. Durée, modification et résiliation de la convention

La présente convention prend effet à compter de sa date de signature, pour une durée indéterminée.

Toute modification des dispositions de la présente convention et des annexes devra faire l'objet d'un avenant signé par les parties.

Elle reste valable tant que l'une ou l'autre des parties ne l'aura pas dénoncée. Si l'une des parties souhaite résilier la présente convention, elle en informe l'autre partie, par écrit, en indiquant les motifs de sa décision. Un préavis de 12 mois est alors nécessaire avant que la résiliation ne soit pleinement effective. Durant cette période, les deux parties s'engagent à assurer le service dans les conditions de cette convention.

Les documents précédemment archivés jusqu'à la date de résiliation resteront archivés durant toute la carrière des personnels de le SITIV et jusqu'à leurs 75 ans ou jusqu'à deux ans après leur décès.

Les stipulations des articles 5 à 9 de la présente convention restent en vigueur après sa cessation pour quelque cause que ce soit.

Fait en deux exemplaires originaux,

A Vénissieux , le 18 mars 2025 Pour le SITIV Monsieur Stéphane Vangheluwe DGS	A Nantes, le Pour la Direction générale des Finances publiques Monsieur David KARLE Sous-directeur, responsable du département du programme de modernisation Service des retraites de l'État

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

Annexe 1

Qualité de service Portail ENSAP :
Le niveau de disponibilité est dit "fort" au sens DGFIP. Ainsi, les exigences pour ce niveau de disponibilité sont les suivantes :

- Portail : ouvert toute l'année.
- Périodes sensibles identifiées : premiers jours de chaque mois, ainsi que lors de la période de délivrance de l'attestation fiscale
- Plages d'ouverture du service pour les usagers : 22h/24h 7/7j. Maintenance réservée plage 01h00 et 03h00
- Accessible via internet
- Pas de besoin d'astreintes les soirs et les week-end.
- Garantie du temps de rétablissement en cas d'incident estimée à 8 heures ouvrées.
- Taux de disponibilité des plages de couverture : 97 %.
- Navigation adaptée à tout support (PC, smartphone, tablettes), compatibilité avec de nombreux navigateurs internet.

Annexe 2

La DGFiP opère un cloisonnement strict des différents réseaux qui composent son SI, conformément aux principes de base recommandés par l'ANSSI. Ce cloisonnement réseau vise à protéger le système d'information et les données qui y sont stockées et traitées, en découpant notamment différents sous-ensembles selon leur sensibilité, tout en y apportant des infrastructures de détection, de contrôle et de traçabilité dédiées.

L'administration de tous les équipements (réseau et applicatifs) est notamment faite au travers d'un réseau dit « d'administration » dédié, totalement décorrélé des réseaux bureautiques.

Les accès aux applicatifs ENSAP seront authentifiés et tracés au travers de dispositifs d'accès et de contrôle, basés sur des annuaires centralisés. Le niveau de privilège associé aux accès est aussi défini au niveau de ces annuaires pour ce qui est de la population agents DGFiP. Les accès usager sont aussi authentifiés et tracés.

Annexe 3

Les mesures de sécurités relatives à l'accès physique au bâtiment et protection des machines

- Sécurité générale des établissements des services informatiques de la DGFiP.

- Sécurité physique des matériels et de l'accès aux informations :

✓ Protection incendie : Les établissements sont dotés de moyens de détection d'incendie avec alarme et/ou déclenchement de dispositifs automatiques d'extinction.

✓ Protection contre les agressions et les vols : les établissements font l'objet d'un renforcement des protections périmétriques (clôtures…) et rapprochées (vitrages anti-effraction…) et sont directement reliés avec le commissariat de police le plus proche.

Pendant les heures de travail, l'accès à l'établissement est contrôlé (badges et registre pour les visiteurs).
La nuit, l'établissement est :
- soit surveillé par un veilleur de nuit ;
- soit fermé et gardé par un système de télésurveillance.
Les jours non ouvrés, l'établissement est :
- soit fermé et gardé par un gardien concierge logé sur place
- soit fermé et gardé par un système de télésurveillance.
L'accès à la salle ordinateur est limité aux seules personnes autorisées par système de badge et les bandothèques sont toujours fermées à clé, sous la responsabilité du chef bandothécaire ou du chef d'exploitation.

- Machines localisées dans un Service de Production Sécurisé (SPS)

L'application est installée dans une salle blanche du site d'hébergement. Ce site présente les caractéristiques suivantes en matière de sécurité :

✓ Détection incendie ;
✓ Extinction incendie ;
✓ Gestion Technique du Bâtiment (GTB) ;
✓ Contrôle d'accès ;
✓ Vidéosurveillance ;
✓ Contrôle anti-intrusion.

La sécurisation du site a été prise en compte dès sa conception tant dans sa dimension passive qu'active :

La sécurisation passive concerne les dispositions constructives prises sur l'architecture et la structure du site et permet d'assurer :

✓ la protection des locaux contre des agressions venant de l'extérieur,
✓ l'impossibilité ou le ralentissement d'une intrusion abusive dans les différentes zones protégées intérieures,
✓ la protection des ouvertures dans les parois nécessaires au fonctionnement des équipements techniques, comme les prises d'air et les rejets, ainsi que les équipements nécessairement disposés à l'extérieur (dry-cooler, par exemple).

La sécurisation active concerne les dispositifs de contrôle, de détection et de surveillance mis en place sur le site. Elle permet de suivre en temps réel l'évolution d'une personne à l'intérieur ou à l'extérieur du bâtiment. Elle intègre :

✓ le contrôle d'accès extérieur et intérieur,
✓ la surveillance / détection par caméras vidéo,
✓ le contrôle d'intrusion.

Pour répondre aux objectifs de sécurité, le site a été organisé en différentes zones présentant des caractéristiques de sécurité adaptées aux enjeux. Le but est d'empêcher l'accès non autorisé au centre informatique et limiter l'impact d'une malveillance ou d'un incendie sur les systèmes d'information.

Les infrastructures de traitement de l'information cruciales ou sensibles sont situées dans une zone limitée par un périmètre de sécurité défini, avec des barrières de sécurité et des mesures de contrôle appropriées à l'entrée. Elles sont protégées physiquement contre les menaces définies. La protection physique est obtenue en créant plusieurs barrières physiques autour du centre informatique.

Trois zones de sécurité seront établies, chacune d'entre elles augmentant la protection totale fournie.

- ✓ Zone Campus : cette zone est définie par la clôture périphérique du terrain. L'accès au campus s'effectue exclusivement sous contrôle du gardien au travers d'un accès véhicule et un accès piétons ;
- ✓ Zone d'accueil : cette zone est définie par l'atrium limité par son enceinte vitrée. Elle constitue une zone de transition entre la zone Campus et la zone Bâtiments. Elle est placée sous contrôle permanent d'un gardien ;
- ✓ Zone bâtiment : cette zone est définie par l'enceinte des trois bâtiments. La zone est limitée par les murs extérieurs, la toiture constituée d'un bac acier supportant une isolation par laine de roche et une étanchéité par revêtement goudronné et enfin au sol la dalle béton. Les ouvrants de la façade sont maintenus fermés par des fixations indémontables. Les baies et ouvrants sont condamnés par l'intérieur, par un bardage acier fixé sur la structure béton. Les issues de secours font l'objet d'une protection mécanique et d'un verrouillage par un dispositif conforme à la réglementation.

L'accès aux bâtiments s'effectue après enregistrement auprès du gardien à la zone d'accueil. L'accès aux bâtiments 1 et 2 renfermant les locaux informatiques fait l'objet d'un contrôle par badge. L'accès est équipé d'un sas. L'accès aux zones informatiques est contrôlé par badge.

Quatre populations accèdent au site :

- ✓ les personnels informatiques,
- ✓ les personnels techniques,
- ✓ les personnels de gardiennage,
- ✓ les visiteurs.

Pour assurer la sécurité du centre ainsi que leur propre sécurité, les personnels et visiteurs doivent se soumettre à tous les contrôles et procédures requises par le plan de sécurité. Le port du badge visible est obligatoire et les personnels sont encouragés à interroger tout visiteur sans escorte ou toute personne ne portant pas d'identification visible.

En matière de sécurité intrusion, aucun signe extérieur ne marque la présence du centre informatique ou ne révèle l'identité de l'occupant. La signalétique est anonyme et ne permet pas de déduire l'activité du centre. L'éclairage est diffus, les dispositifs de surveillance extérieure (détecteurs, caméras…) discrets. Aucun véhicule ne doit stationner en dehors des zones parking. L'arrêt sur les zones livraison est limité au temps nécessaire au chargement ou au déchargement.

Les zones de services (photocopieurs, télécopieurs) et les commodités sont en dehors des zones informatiques ou techniques. A chaque périmètre de sécurité est mise en œuvre une surveillance électronique :

- ✓ Zone Campus : La clôture extérieure est équipée d'une détection de chocs sur clôture et de contacts d'ouverture sur les portails et portillons. Les accès extérieurs et les zones extérieures font l'objet d'une vidéosurveillance.
- ✓ Zone bâtiment : Les baies, ouvrants et issues de secours situés au rez-de-chaussée sont surveillées par une détection choc et ouverture. Les toitures sont surveillées par des barrières infra-rouge couplées au système de vidéosurveillance couvrant la zone. Les salles informatiques sont mises sous contrôle du système de vidéosurveillance. Les locaux inoccupés sont fermés à clef et mis sous contrôle du système de vidéosurveillance. Les circulations et le hall d'accueil font l'objet d'une vidéosurveillance. Les accès contrôlés par badge sont surveillés par contact de choc et ouverture (effraction et porte restée ouverte trop longtemps).

En matière de sécurité incendie, les moyens mis en œuvre sont les suivants :

- ✓ Moyens préventifs : Les zones informatiques sont isolées par une enceinte séparative coupe-feu 2 heures étanche aux fumées et aux fluides. Les salles informatiques sont maintenues en surpression pour éviter une contamination par des fumées venant de l'extérieur. Les armoires techniques climatisation et électricité sont placées dans les couloirs techniques à l'extérieur des zones informatiques. Les matières dangereuses ou inflammables sont stockées en sûreté, à distance des zones informatiques. Les fournitures telles que papier ou supports magnétiques sont stockées en dehors des zones informatiques.
- ✓ Moyens curatifs : Le processus comporte 3 étapes :
  - ✓ Détection automatique rapide et fiable favorisant la réactivité des intervenants ;
  - ✓ Déconnexion de la machine en défaut ou utilisation d'extincteurs portables CO2 ou H2O ;
  - ✓ Recours à une extinction automatique.

Envoyé en préfecture le 26/05/2025
Reçu en préfecture le 26/05/2025
Publié le
ID : 069-256910183-20250523-CS_2025_05_4-DE

Annexe 4

L'ENSAP s'inscrit dans la politique de sécurité de la DGFiP dont l'AQSSI est le garant.
L'application bénéficie à ce titre comme l'ensemble des projets de la DGFiP :

- d'une démarche formelle d'amélioration continue de la sécurité
- d'une sécurisation des données traitées
- d'une détection et gestion des incidents de sécurité
- d'une promotion des mesures de sécurité auprès des utilisateurs
- d'une identification et gestion des risques
- d'un plan de reprise d'activité (PCA) testé régulièrement
- d'un maintien en condition opérationnelle
- d'une homologation par la DGFiP de l'application ENSAP en conformité avec les normes imposées par le RGS. (calendrier et modalités à définir par la DGFIP)

Le SITIV participe à la sécurité du projet en :

- étant destinataire de la politique de sécurité retenue
- respectant les règles d'emploi et de sécurité afférentes au SI ENSAP émanant de la DGFIP,
- dé-sensibilisant les données véhiculées dans les flux, si nécessaire (ex. : suppression de l'adresse postale des usagers),
- chiffrant les échanges et les données
- détectant et gérant les incidents de sécurité sur son système d'information dont il a la maîtrise d'œuvre
- faisant la promotion des mesures de sécurité auprès des utilisateurs
- respectant le format d'échange des données sous peine de rejet de l'intégralité du flux.