ACCES AU SI DE FRANCE TRAVAIL PAR DES TIERS

RÈGLES DE SÉCURITÉ

Référence	FT_SSI-REG-TST_Accès au SI de FT par des tiers_V2
Clef GED	72649
Version	V2
Classification	Interne
Date	15/01/2021
État	Validé
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	RSSI : Sylvain Lambert
Validation	Direction de la Maîtrise des Risques

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de France Travail

Diffusion interne

Identification du document

Référence	Titre du document	
FT_SSI-REG-TST_Accès au SI de FT par des tiers_V2	Accès au SI de FT par des Tiers	
Version	**État du document**	**Auteurs**
2	Final	Filière Sécurité des SI

Classification

Niveau	Diffusion
Interne	Le personnel de France Travail et à ses tiers formellement autorisés (ayant signé une convention, charte de sécurité, clause de confidentialité,…)

Mises à jour

Version	Date	Nature de la modification
1.0	05 février 2009	Création du document
1.6	25 mars 2013	Relecture thématique SSI – groupe de travail filière SSI
1.8	26 avril 2017	Mises à jour dans le cadre de la refonte du référentiel initiée en 2016
1.9	04 juin 2020	Mises à jour dans le cadre de la directive NIS (conformité OSE)
1.9	15 janvier 2021	Ajout de la nécessité de répondre aux exigences de sécurité au travers un PAS (plan assurance Sécurité)
2	22 janvier 2024	Mise à jour suite changement de marque

Relectures et validations

Version	Relu par	Direction	Date	Statut
1.0	RSSI Mylène Zerbib	DSI	10/06/2009	validé
1.6	RSSI Sylvain Lambert	DSI	25/03/2013	validé
1.8	RSSI Sylvain Lambert	DSI	26/04/2017	validé
1.8	Robert Laupy	DMR	29/06/2017	validé
1.9	RSSI Sylvain Lambert	DSI	17/07/2020	validé

Documents de référence

Référence colibri	Titre du document
Colibri 262372	Environnement de travail - Fixes
Colibri 262373	Environnement de travail - Mobiles
Colibri 72624	Contrôle des accès logiques - Utilisateurs

SOMMAIRE

1. REGLES GENERALES DE SECURITE 4
1.1. Sécurité d'ensemble 4
1.2. Confidentialité des informations 4
1.3. Détournement de finalité 4
1.4. Coordination des travaux et de la sécurité 4
1.5. Personnel utilisé 4
1.6. Sensibilisation à la sécurité 5
1.7. Politique de Sécurité 5
1.8. Convention de Service 5
1.9. Respect des dispositions « Informatique et libertés » 5
2. ACCES AUX MOYENS INFORMATIQUES 6
2.1. Réseau 6
2.2. Application (interconnexion applicative) 6
2.3. Infrastructure distante 8
2.4. Identification / Authentification 8
2.5. Poste de travail 10
2.6. Audit et Contrôle 10

1. RÈGLES GÉNÉRALES DE SÉCURITÉ

1.1. SÉCURITÉ D'ENSEMBLE

- Le titulaire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations. Il veillera notamment à empêcher qu'elles soient déformées, endommagées ou communiquées à des tiers non autorisés et ce, de façon intentionnelle ou accidentelle.
- Le titulaire doit maintenir opérationnels les dispositifs de sécurité qu'il s'engage à mettre en place. Il doit informer sans délai France Travail de tout déménagement ou modification d'implantation.
- Les informations fournies par France Travail ne doivent pas être considérées comme une cession ou un échange. Elles restent la propriété de France Travail, ainsi que celles qu'il crée pour le compte de celui-ci.
- Les dispositions prises par le prestataire pour répondre aux exigences de sécurité du présent document devront être formalisées au sein d'un PAS (Plan d'Assurance Sécurité).

1.2. CONFIDENTIALITÉ DES INFORMATIONS

- Quel qu'en soit leur support (physique ou électronique), le titulaire doit considérer comme confidentielles toutes les informations qu'il reçoit de France Travail, traite ou crée pour le compte de celui-ci. Le stockage et le traitement des informations de France Travail doivent être réalisés de manière à prévenir la perte, la modification comme la mauvaise utilisation des données de France Travail.

1.3. DÉTOURNEMENT DE FINALITÉ

- Aucun autre traitement que ceux prévus contractuellement ne doit être exécuté sur ces informations ou leurs résultats. Tout traitement doit être adapté au but pour lequel il a été mis en place et ne doit pas servir d'autres fins.
- Le titulaire s'interdit l'utilisation des moyens et ressources informatiques mis à sa disposition par France Travail à des fins autres que celles figurant dans le contrat.

1.4. COORDINATION DES TRAVAUX ET DE LA SÉCURITÉ

- Un employé du titulaire sera désigné pour coordonner et superviser les travaux sur le plan technique et contrôler l'application des règles de sécurité demandées par France Travail. Il assure l'interface entre l'entreprise et France Travail. Il doit notamment être présent lors des éventuels contrôles de sécurité effectués par France Travail.

1.5. PERSONNEL UTILISÉ

- Le titulaire ne peut confier tout ou partie des travaux de France Travail à l'un de ses

sous-traitants ou de les faire effectuer par du personnel intérimaire, sauf s'il en a obtenu l'accord écrit et préalable de France Travail.

1.6. SENSIBILISATION À LA SÉCURITÉ

- Le titulaire donne à son personnel une formation portant sur les règles de sécurité à observer.
- Il fait signer à ses intervenants l'engagement de confidentialité communiqué par France Travail.

1.7. POLITIQUE DE SÉCURITÉ

- Le titulaire devra communiquer à France Travail sa politique SSI. Celle-ci doit être compatible et en cohérence avec les exigences exprimées par celle de France Travail.

1.8. CONVENTION DE SERVICE

- Le titulaire s'engage à respecter des conditions de service contractuelles, notamment en cas de télémaintenance, télé administration, etc. Ces conditions reposent notamment sur la disponibilité des équipements et équipes du titulaire.
- Le cas échéant, le titulaire devra présenter ou décrire à France Travail son plan de secours en cas de sinistre pouvant affecter les travaux réalisés pour France Travail.

1.9. RESPECT DES DISPOSITIONS « INFORMATIQUE ET LIBERTÉS »

- Le titulaire garantit qu'il traitera les données à caractère personnel conformément à la loi et aux décrets applicables, notamment en ce qui concerne la sécurité et la confidentialité des dites données.
- Il a connaissance de l'existence du règlement européen sur la protection des données à caractère personnel, relatif à l'informatique, aux fichiers et aux libertés, qui pourraient s'appliquer à tout manquement de sa part mettant en jeu des données à caractère personnel.

2. ACCÈS AUX MOYENS INFORMATIQUES

Lorsqu'il accède à des moyens informatiques de France Travail, le titulaire s'engage à appliquer les règles de sécurité suivantes :

2.1. RÉSEAU

2.1.a Tout accès logique au réseau de France Travail est contrôlé par un système d'identification et d'authentification conforme aux règles édictées dans le paragraphe *2.4 Identification / Authentification*.

2.1.b Sauf dérogation explicite acceptée par le RSSI de France Travail, tous les flux entre le Système d'Information du titulaire et ceux de France Travail transitent obligatoirement par le PAE (Point d'Accès Externe) de France Travail.

2.1.c Un système de détection des tentatives d'accès logiques non autorisés sur le Système d'Information du titulaire doit être en place pour prévenir toute intrusion. En outre, un système de filtrage des codes malveillants (virus, vers, etc.) doit être en place entre le titulaire et France Travail. Toute alerte, provenant de ces systèmes, doit être remontée à France Travail.

2.1.d Le descriptif de l'interconnexion technique avec la matrice de flux identifiant les protocoles entre le titulaire et France Travail doivent être fournis à France Travail.

2.2. APPLICATION (INTERCONNEXION APPLICATIVE)

2.2.a Chaque serveur du titulaire accédant au Système d'Information de France Travail doit être sécurisé conformément à une Politique de Sécurité des SI compatible et en cohérence avec les exigences exprimées par la Politique de Sécurité des SI de France Travail (Ex : Système d'habilitations, correctifs de sécurité & anti-virus à jour, protection des données, contrôle d'intégrité, etc.).

2.2.b Chaque serveur du titulaire accédant au Système d'Information de France Travail doit être supervisé, administré et contrôlé à intervalles réguliers.

2.2.c Un descriptif de l'interconnexion applicative ainsi qu'une spécification des flux *fonctionnels* entre les ressources du titulaire et celles de France Travail doivent être fournis à France Travail.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de France Travail

Diffusion interne

2.3. INFRASTRUCTURE DISTANTE

2.3.a Dans le cas d'un titulaire travaillant pour France Travail et en dehors des locaux de France Travail, l'infrastructure du titulaire lui permettant d'accéder au Système d'Information de France Travail doit bénéficier d'un dispositif de sécurité physique. Les zones sensibles permettant cette interconnexion regroupant les infrastructures d'interconnexion doivent être des zones à accès restreint.

2.3.b Dans le cas de sauvegardes de données effectuées par le titulaire :

- Le titulaire doit réaliser des sauvegardes sous réserve que le mode de duplication ait été agréé par France Travail et décrit dans le contrat.
- Il doit protéger les sauvegardes comme les éléments originaux, afin d'éviter toute possibilité d'accès, fortuit ou intentionnel, par des tiers ou des employés non autorisés.
- Les conditions de restitution de ces sauvegardes à France Travail ou de destruction par un mode agréé par France Travail, doivent être prévues au contrat, en accord avec France Travail.
- Les supports magnétiques amovibles contenant des données de France Travail doivent être identifiés, protégés contre tout accès non autorisé et périodiquement inventoriés.

2.4. IDENTIFICATION / AUTHENTIFICATION

2.4.a Les droits d'accès des intervenants extérieurs sont gérés directement par le responsable fonctionnel de France Travail pour lequel ils interviennent. Ce dernier est chargé de gérer le cycle de vie de l'intervenant, depuis la signature jusqu'à la fin du contrat : enregistrement en tant qu'utilisateur des SI, habilitations sur la base des missions qu'il lui confie ; suivi de ces habilitations, révocation des droits en fin de mission. Un contrôle d'accès logique aux données de France Travail doit être en place pour permettre de distinguer les différents types d'accès (lecture, mise à jour, exécution) et garantir qu'elles ne sont accessibles qu'aux seules personnes préalablement autorisées. La liste de ces personnes doit faire l'objet d'une mise à jour permanente et doit être communiquée régulièrement à France Travail. Les accès devront être révoqués immédiatement en cas de cessation du besoin de l'utilisateur.

2.4.b Les autorisations d'accès aux ressources du SI de France Travail sont strictement personnelles et ne peuvent en aucun cas être cédées à un tiers.

Lorsque l'authentification des utilisateurs se fait par mot de passe ou par identité numérique, celle-ci doit rester confidentielle. Tout comme l'identifiant, elle est personnelle, unique et intransmissible. Il appartient donc à chaque utilisateur de préserver sa confidentialité. Pour un mot de passe, il doit être choisi au hasard de telle sorte qu'il ne soit ni évident, ni prévisible ou vulnérable à des tentatives répétées d'accès frauduleux.

2.4.c Toute demande d'habilitation doit préciser une date d'expiration correspondant normalement à la date de fin de contrat. Les demandes sont transmises au responsable des habilitations de l'entité fonctionnelle concernée de France Travail, qui est chargé d'assurer l'interface avec l'administrateur opérationnel des droits de France Travail.

2.4.d Plus généralement, les règles, édictées dans le document thématique Sécurité « Contrôle des accès logiques » fourni après notification du marché par France Travail, doivent, lors d'une authentification sur une ressource de France Travail, être respectées et notamment concernant la construction de l'authentifiant (le mot de passe) qui doit obéir aux critères de qualité qui y sont spécifiés :

- Avoir une longueur minimale de 8 caractères,
- Être composé de caractères appartenant aux trois classes suivantes : lettres (a…z et A...Z), chiffres (0...9) et caractères spéciaux (&@à(|...),,
- Être changé régulièrement au moins tous les 3 mois, etc.

2.4.e En cas de mise en œuvre d'une communication application à application, une authentification forte est requise. Les modalités pratiques de déclinaison de ces principes seront adaptées au cas par cas en fonction des contraintes identifiées.

2.4.f Phase de connexion au Système d'Information de France Travail : Pour les prestataires ex situ, les intervenants doivent s'authentifier sur l'infrastructure de sécurité positionnée en frontière du Système d'Information de France Travail.

2.5. POSTE DE TRAVAIL

2.5.a Les terminaux ne doivent pas rester en session en dehors de la présence de l'utilisateur à son poste de travail (procédure de déconnexion – *logoff* ou de mise en veille).

2.5.b L'utilisateur doit quitter son poste de travail en se déconnectant, ce qui permet de rendre les ressources ou les services inaccessibles.

2.5.c L'utilisateur doit signaler immédiatement à son responsable hiérarchique toute anomalie ou tentative d'intrusion ou de violation concernant son poste de travail.

2.5.d Lorsqu'il se connecte au réseau de France Travail, le titulaire s'engage à n'utiliser que des postes respectant les règles du document thématique Sécurité « Environnements de travail Fixe et/ou Mobiles » (équipement physique ou virtuel). L'accès à des ressources partagées France Travail depuis un poste tiers nécessite l'installation d'un composant logiciel d'authentification labellisé par France Travail (kit prestataire).

2.5.e Le poste de travail tiers (physique ou virtuel) doit être équipé :

- D'un système d'exploitation à jour et supporté par l'éditeur,
- D'un dispositif de prévention, détection et d'éradication des virus informatiques, dont le moteur et la base virale sont à jour.
- D'un module vérifiant son niveau de sécurité (niveau de mise à jour anti-virale) avant la phase d'authentification.
- Pour des besoins spécifiques d'accès distant au SIE, France Travail pourra exiger la protection des mémoires de masse du poste de travail accédant ou rebond, par des mécanismes de chiffrement conforme aux préconisations de l'ANSSI.

2.5.f Lorsqu'elles sont utilisées pour la production d'informations de France Travail, les imprimantes doivent être protégées de tout accès non autorisé, soit par surveillance visuelle, soit en étant placées dans une zone à accès restreint et contrôlé.

2.5.g Tous les intervenants extérieurs reçoivent un exemplaire des règles d'utilisation des systèmes d'information et de communication de France Travail et signent un engagement de confidentialité.

2.6. AUDIT ET CONTRÔLE

2.6.a Les équipements mis à disposition des collaborateurs du prestataire leur permettant de réaliser leurs missions pour le compte de France Travail, doivent faire l'objet de mesures spécifiques de protection pour empêcher leur

utilisation, leur modification, leur reproduction non autorisée. Ces mesures doivent comprendre :

- Des procédures formelles et des traces complètes des activités,
- Des accès limités dans le temps, uniquement aux utilisateurs habilités et pour effectuer des travaux spécifiquement autorisés,
- Des contrôles réguliers de l'utilisation, par le management hiérarchique.

2.6.b Le titulaire devra effectuer périodiquement des revues impromptues pour vérifier la conformité avec les dispositions du présent accord.

2.6.c France Travail est autorisé à vérifier, dans les locaux du titulaire, par des visites programmées ou non, la bonne application du présent accord.

2.6.d Le titulaire s'engage à informer immédiatement France Travail de tout événement pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la perte d'informations de France Travail qu'il détient. Il a le devoir d'avertir France Travail en cas de tentatives d'accès logiques non autorisées, intrusions, activités malveillantes de toute nature, détectées sur son site. En outre, le titulaire s'engage à informer immédiatement France Travail de toute modification de l'infrastructure distante.

2.6.e En accord avec le titulaire, France Travail peut vérifier la conformité des flux avec les déclaratifs fournis.