# EXIGENCES DE SECURITE APPLIQUEES AUX TIERS

## REGLES DE SECURITE

| | |
|---|---|
| Référence | SSI-REG-TST_Exigences de sécurité appliquées aux tiers V1.2 |
| Clef GED | 72641 |
| Version | V1.3 |
| Classification | Interne |
| Date | 15/01/2021 |
| État | Final |
| Auteur(s) | Filière Sécurité des SI |
| Approbateur(s) | Sylvain Lambert |
| Validation | Direction Maitrise des Risques |

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

Diffusion interne

## Identification du document

| Référence | Titre du document | |
|---|---|---|
| SSI-REG-TST_Exigences de sécurité appliquées aux tiers V1.2 | Exigences de sécurité appliquées aux tiers | |
| **Version** | **État du document** | **Auteurs** |
| 1.3 | 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 |
|---|---|---|
| 0.1 | 03 Mars 2008 | Création du document |
| 1.0 | 10 juin 2009 | Version finale |
| 1.1 | 05 février 2015 | Modification mineure TST-02 pour adéquation avec la DdA |
| 1.11 | 06 juillet 2017 | Mises à jour dans le cadre de la refonte du référentiel initiée en 2016 |
| 1.2 | 14 décembre 2017 | Version finale |
| 1.2 | 15 janvier 2021 | Ajout de la nécessité de répondre aux exigences de sécurité au travers un PAS (plan assurance Sécurité) |
| 1.3 | 22 janvier 2024 | Mise à jour suite changement de marque |

## Relectures et validations

| Version | Relu par | Direction | Date | Statut |
|---|---|---|---|---|
| 1.0 | | DGA-DMR | 10 juin 2009 | validé |
| 1.1 | COPIL SSI | DGA-SI | 04/02/2014 | validé |
| 1.1 | | DGA-DMR | 15/03/2014 | validé |
| 1.2 | RSSI Sylvain Lambert | DGA-SI | 14/12/2017 | validé |
| 1.2 | Mojdeh Hodjat-Panah-Daurelle | DGA-DMRS | *Absence de retour au 24 mai 2018* | |

## Documents de référence

| Référence | Titre du document |
|---|---|
| *[1] Colibri 196557* | Demande de dérogation |
| *[2] Colibri* 72649 | Accès au SI de FT par des Tiers |
| *[3] Colibri* 185487 | Partenariat – Echange de données |
| *[4] Colibri* 273304 | Hébergement Services en ligne ou Cloud |
| *[5] Colibri* 268674 | Engagement individuel de confidentialité |



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

Diffusion interne

| | |
|---|---|
| *[6] Colibri* 198667 | Externalisation de donnée – Questionnaire Sécurité |



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

Diffusion interne

# SOMMAIRE

**1. PREAMBULE ..... 5**
1.1. Principes fondateurs de la Politique Générale de Sécurité des SI ..... 5
1.2. Enjeux et objectifs du document ..... 5
1.3. Champ d'application ..... 6
**2. CONCEPTS GENERAUX ..... 7**
2.1. Définition ..... 7
2.2. Types de prestations et types d'accès identifiés pour les tiers ..... 7
**3. ROLES ET RESPONSABILITES ..... 8**
**4. DOCUMENTATIONS SUPPORT ..... 9**
**5. REGLES DE SECURITE ..... 12**
**6. ANNEXES ..... 15**
6.1. Glossaire ..... 15
6.2. Liste des règles ..... 16

***Règles typographiques***

Les termes écrits en vert et soulignés sont définis dans le glossaire de ce document.

Les règles de la thématique « Exigence de sécurité appliquées aux tiers » sont préfixées par le sigle « **TST**- » et sont numérotées par ordre d'apparition. Elles sont définies dans un encart bleu clair comme figuré ci-dessous :

| |
|---|
| *Définition de la règle* |

Pour certaines règles, des préconisations, recommandations, commentaires ou des évolutions prévisibles sont détaillés au-dessous de la règle.

**Préconisations :**

La maîtrise d'œuvre est orientée vers une solution pour couvrir la règle de sécurité.

**Recommandations :**

L'utilisateur est orienté vers un comportement, un usage, afin de respecter la règle de sécurité.

**Commentaires :**

Des précisions sont apportées afin d'éclairer la règle énoncée.



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

Diffusion interne

# 1. PRÉAMBULE

## 1.1. PRINCIPES FONDATEURS DE LA POLITIQUE GÉNÉRALE DE SÉCURITÉ DES SI

Les Systèmes d'Information hébergent de nombreuses données qui revêtent un caractère stratégique et qui constituent un patrimoine essentiel que France Travail a l'obligation de protéger efficacement.

Pour ce faire, la Direction adopte une Politique Générale de Sécurité des SI qui s'inscrit dans le cadre de la politique de gestion des risques ; cette politique protège les informations et leurs traitements ainsi que les ressources hébergées par les Systèmes d'Information de France Travail.

## 1.2. ENJEUX ET OBJECTIFS DU DOCUMENT

Afin d'assurer la gestion optimale de ses Systèmes d'Information, France Travail a recours à des prestations de tiers.

Le recours à des prestations de tiers induit de nouveaux risques au niveau des Systèmes d'Information, en particulier :

- Des risques d'atteinte à la disponibilité des informations et des traitements, notamment pour ce qui concerne les prestations d'hébergement ou d'infogérance de composants des Systèmes d'Information,
- Des risques liés à la divulgation ou la perte (de données, d'intégrité, de preuve…), au travers notamment d'interconnexions des SI avec des systèmes partenaires, ou via le recours à des prestations externalisées (développement, exploitation, etc.) traitant des informations sensibles,
- Des risques juridiques, notamment pour ce qui concerne le développement des sites et/ou services internet, dont France Travail est responsable,
- Des risques de fraude ou de malveillance par des acteurs externes à France Travail.

Ces risques sont aggravés par le fait que les utilisateurs ne sont pas sous le contrôle juridique de France Travail, qu'ils ne sont pas toujours sous contrôle physique et que les accès peuvent se faire à partir de locaux extérieurs et de Systèmes d'Information extérieurs.

Le présent document traite :

- De l'intégration de mesures de sécurité dans tous les services sous-traités à des tiers,
- De la protection des échanges d'informations avec les tiers,
- De la protection de l'accès par les tiers aux informations et Systèmes d'Information de France Travail.

Les principes du présent document sont détaillés dans les documentations support suivantes :

- « Accès au SI de France Travail par des tiers » [2],
- « Partenariat – Echange de données » [3],
- « Hébergement Services en ligne ou Cloud » [4],
- « Engagement individuel de confidentialité » [5],
- « Externalisation de données – Questionnaire Sécurité » [6].



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

Diffusion interne

## 1.3. CHAMP D'APPLICATION

Ce document concerne tous les acteurs amenés à engager et piloter des prestations de tiers,

Celui-ci :

- Introduit et présente les documentations support qui définissent les exigences de sécurité applicables aux tiers selon la nature de la prestation, à inclure dans le contrat,
- Définit les règles générales de sécurité permettant de maîtriser les risques potentiels induits par les interventions de tiers.

En cas de non applicabilité d'une des règles du présent document, une procédure de dérogation doit être engagée. Cette demande de dérogation [1] sera transmise au Responsable Sécurité des Systèmes d'Information.

Les dispositions prises par le tiers pour répondre aux exigences de sécurité qui lui sont applicables devront être formalisées au sein d'un PAS (Plan d'Assurance Sécurité).



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

Diffusion interne

# 2. CONCEPTS GÉNÉRAUX

## 2.1. DÉFINITION

Le terme « tiers » désigne l'ensemble des stagiaires, des prestataires, des fournisseurs, des partenaires et des travailleurs intérimaires amenés à travailler, de manière permanente ou occasionnelle, sur les Systèmes d'Information et, de ce fait, à avoir accès potentiellement aux informations ou ressources de France Travail.

## 2.2. TYPES DE PRESTATIONS ET TYPES D'ACCÈS IDENTIFIÉS POUR LES TIERS

Les interventions de tiers sur les Systèmes d'Information peuvent être de différents types, et notamment :

- Des prestations intellectuelles (missions de conseil, d'analyse, d'étude, d'audit, etc. qui ne comportent pas de fourniture de produits matériels),
- Des prestations de développement de logiciel,
- Des prestations d'infogérance, d'externalisation, d'hébergement,
- Des prestations de maintenance applicative de type MCO (Maintien en Conditions Opérationnelles) ou TMA (Tierce Maintenance Applicative),
- Des prestations de maintenance de matériels et/ou de logiciels,
- Des prestations de location, d'achat et d'intégration de matériels et/ou de logiciels,
- Des prestations métiers dans le cadre de partenariats.

Les interactions entre les Systèmes d'Information du tiers avec ceux de France Travail peuvent être de différents types :

- Accès d'un tiers depuis des locaux internes de France Travail.
- Accès depuis des locaux externes à France Travail :
  - Accès interactif d'un tiers depuis un site distant externe (exemple : opérations de maintenance, accès partenaires),
  - Communication application à application (ex : transfert de fichiers, web services, etc.).



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

Diffusion interne

# 3. RÔLES ET RESPONSABILITÉS

Le présent chapitre a pour but de définir les fonctions intervenant dans la gestion des tiers. Ces fonctions regroupent des missions et des responsabilités qui correspondent à un ou plusieurs acteurs.

- Le Responsable de contrat (Maîtrise d'Ouvrage, Métier, etc.)
  - Identifie, avec l'appui de la Maîtrise d'Ouvrage Sécurité, les risques de Sécurité SI induits par la prestation et détermine les exigences de sécurité,
  - Valide les mesures de sécurité spécifiques (contractuelles ou opérationnelles) à mettre en place pour parer ces risques,
  - Rédige ou valide le contrat avec le tiers, et veille à sa conformité avec le niveau de risque, les règles du présent document et ses déclinaisons présentes dans les documentations support associés à la prestation.,
  - Informe le Correspondant Sécurité (RSI-Op) de sa Direction du suivi et de l'avancement des actions relatives à la sécurité dans le cadre du contrat,
  - Veille, notamment par des actions de sensibilisation et de contrôle, à ce que les mesures de sécurité identifiées soient mises en œuvre (gestion des habilitations, gestion des incidents, suivi des engagements de service, etc.),
  - Veille à la prise en compte de la Sécurité des SI en cas de fin ou de terminaison de la prestation (suppression des accès, restitution ou destruction des informations, etc.).
- La Maîtrise d'Ouvrage Architecture
  - Est chargée de la définition des architectures techniques d'interconnexion avec les tiers,
  - Assiste la Maîtrise d'Œuvre pour décliner les exigences de sécurité en mesures.
- La Maîtrise d'Ouvrage Sécurité
  - Accompagne la Maîtrise d'Ouvrage ou le Métier dans la définition des exigences de sécurité,
  - Participe à la définition des mesures à mettre en place dans le cadre d'une prestation de tiers,
  - Conduit des actions de contrôle de la Sécurité SI sur le périmètre du tiers.
- La Maîtrise d'Œuvre
  - Est chargée de la mise en place des architectures d'interconnexion avec les tiers, et de leur maintien en conditions opérationnelles,
  - Est chargée de la mise en place des mesures de sécurité.
- Les Utilisateurs tiers
  - Respectent les règles de sécurité qui les concernent, notamment les règles de sécurité relatives à l'utilisation des Systèmes d'Information et de communication de France Travail ainsi que les règles spécifiques figurant au contrat.



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

Diffusion interne

# 4. DOCUMENTATIONS SUPPORT

Ce chapitre a pour but de présenter les enjeux et objectifs des documentations support associées au présent document.

- « Accès au SI de France Travail par des tiers » [1]
  - Ce document énumère les exigences de sécurité applicables dans le cas d'accès au SI de France Travail par des tiers.
  - Les exigences de ce document ont vocation à être intégrées dans l'accord contractualisé avec le tiers.

- « Partenariat – Echange de données » [2] ;
  - Ce document énumère les exigences de sécurité sur lesquelles le co-contractant (partenaire de France Travail ou un sous-traitant de France Travail) devra s'engager dans le cadre d'un partenariat d'échange de données avec France Travail.
  - Les exigences de ce document ont vocation à être intégrées dans l'accord contractualisé avec le co-contractant mais également dans le cadre du choix du co-contractant, par exemple dans la rédaction du cahier des charges.

- « Hébergement Services en ligne ou Cloud » [3] ;
  - Ce document énumère les exigences de sécurité applicables aux tiers dans le cadre d'une offre de service accessible en ligne ou hébergée en Cloud.
  - Il permet à France Travail de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité de sa prestation et sur la confiance que France Travail peut lui accorder.
  - Les exigences de ce document ont vocation à être intégrées dans l'accord contractualisé avec le tiers.

- « Engagement individuel de confidentialité » [4] ;
  - Cette charte doit être signée nominativement par toute personne travaillant pour le compte d'un tiers intervenant pour France Travail et ayant accès à des données confidentielles.

- « Externalisation de données – Questionnaire Sécurité » [5].
  - Ce document présente un questionnaire sécurité reprenant l'ensemble des points que France Travail, conformément à sa politique générale de sécurité des systèmes d'information, souhaite voir traiter dans le cadre de l'externalisation de ses données, d'un logiciel, d'une plateforme ou d'une infrastructure.
  - Il est intégré à tous les cahiers des charges liés aux contrats de prestation pour lesquels des données de France Travail sont hébergées hors des structures de l'institution.



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

Diffusion interne

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

Diffusion interne

Le tableau ci-après synthétise les éléments mentionnés précédemment :

| Phase | Type de prestation | Nom du document |
|---|---|---|
| Appel d'offres | Service en ligne - Cloud | Externalisation de données – Questionnaire Sécurité |
| | Echange de données | Partenariat – Echange de données |
| Contractualisation | Accès au SI | Accès au SI de France Travail par des tiers |
| | Echange de données | Partenariat – Echange de données |
| | Service en ligne - Cloud | Hébergement Services en ligne ou Cloud |
| Intervention | Toutes | Engagement individuel de confidentialité |



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

Diffusion interne

# 5. RÈGLES DE SÉCURITÉ

## TST-01 Définition des exigences de sécurité

Pour toute intervention de tiers, des exigences de sécurité SI permettant de couvrir les risques induits par la prestation doivent être définies.

Afin d'identifier les exigences de sécurité applicables selon la nature de la prestation et la phase considérée (appel d'offres, contractualisation, intervention), il convient de s'appuyer sur les documentations support présentées au Chapitre 4 du présent document.

***Commentaires :***

Suivant la nature de la prestation et la phase considérée, les exigences de sécurité applicables aux tiers sont détaillées dans les documents suivants :

- « Accès au SI de France Travail par des tiers » [2],
- « Partenariat – Echange de données » [3],
- « Hébergement Services en ligne ou Cloud » [4],
- « Engagement individuel de confidentialité » [5],
- « Externalisation de données – Questionnaire Sécurité » [6].

## TST-02 Contractualisation des interventions des tiers

Toute intervention de tiers doit faire l'objet d'un **contrat**. Celui-ci doit intégrer les exigences de sécurité SI mentionnées précédemment dans la règle TST-01.

Ce contrat est placé sous la responsabilité d'un acteur interne nommément identifié, ci-après appelé le **« responsable du contrat ».**

***Commentaires :***

Le terme contrat doit être entendu au sens large et comprend aussi les conventions de stage, les contrats d'intérimaires, les contrats de prestation, etc.

Le responsable de contrat doit s'assurer, ou faire vérifier par toute personne de son choix, que l'ensemble des règles du présent document et des documentations support est mis en œuvre et que les actions suivantes sont réalisées dans le respect de celles-ci :

- Définition des responsabilités respectives des deux parties,
- Communication des exigences de sécurité aux tiers concernés,
- Communication du niveau de service attendu.



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

Diffusion interne

## TST-03 Engagement de confidentialité et respect des exigences de sécurité

Toute personne intervenant pour le compte du tiers doit être **informée** des consignes de sécurité SI qui la concernent et doit s'engager à les appliquer.

Toute personne travaillant pour le compte du tiers doit signer un **engagement de confidentialité** dès qu'elle intervient pour France Travail. Cela concerne obligatoirement les tiers manipulant ou ayant accès à des informations classifiées à un niveau élevé de confidentialité.

***Recommandation :***

La signature de l' « **Engagement individuel de confidentialité** » déclenche l'initialisation de la demande des droits d'accès aux systèmes d'information de France Travail pour le nouvel intervenant.

## TST-04 Pilotage des interventions des tiers

Durant toute la durée de l'intervention, le responsable du contrat s'assure du **respect des engagements** prévus dans le contrat.

***Commentaires :***

Le responsable de contrat veille notamment à la prise en compte de la sécurité lors des phases de renouvellement de contrat (renouvellement des habilitations, signature des engagements de confidentialité des nouveaux intervenants, etc.).

## TST-05 Validation des accès du tiers au Système d'Information de France Travail

Tout accès au SI de France Travail par un tiers nécessite l'**autorisation préalable** du responsable du contrat concerné (acteur interne).

## TST-06 Inventaire des accès logiques et physiques

Un **inventaire des accès logiques et physiques** accordés à chaque tiers sur les Systèmes d'Information doit être constitué à l'initialisation du contrat et maintenu à jour.

## TST-07 Traçabilité des accès logiques et physiques

Les accès logiques et physiques aux Systèmes d'Information par des tiers doivent être **tracés et journalisés**. Les tiers doivent être informés de cette journalisation.

***Commentaires :***

La durée de conservation de ces traces est conforme aux préconisations de la CNIL.



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

Diffusion interne

## TST-08 Fin d'intervention du tiers

À la fin de l'intervention du tiers, le responsable du contrat veille au respect des exigences de Sécurité SI liées à la **clôture** de celle-ci.

***Commentaires :***

En particulier, il s'assure de la suspension de l'ensemble des accès et habilitations mis à disposition des tiers, ainsi que de la restitution des biens matériels, de la restitution ou la destruction de l'intégralité des documents et données remis au tiers dans le cadre de son intervention.



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

Diffusion interne

# 6. ANNEXES

## 6.1. GLOSSAIRE

| | |
|---|---|
| **Confidentialité** | La confidentialité est la propriété qui garantit que les Informations ne sont accessibles que par des personnes dûment habilitées et qu'elles ne peuvent pas être divulguées en dehors des règles établies.<br>Cette garantie peut être mise en cause par des indiscrétions, volontaires ou involontaires, quel que soit le support utilisé (réseau, CD, etc.). |
| **Disponibilité** | La disponibilité est l'aptitude d'un système d'Information à pouvoir être employé par les utilisateurs (individus, entités, processus…) habilités dans des conditions d'accès et d'usage normalement prévues (conditions d'horaires, de délai, de performances…). |
| **Intégrité** | L'intégrité est la propriété qui assure qu'une Information n'est modifiée que par les utilisateurs habilités dans des conditions d'accès normalement prévues. L'intégrité doit garantir l'exhaustivité, l'exactitude et la fiabilité de l'Information.<br>L'intégrité peut être remise en cause par toute altération ou modification non légitime. |
| **Preuve** | La preuve correspond aux éléments permettant de prouver l'origine des traitements ou autres événements relatifs à un composant des Systèmes d'Information et d'en reconstituer le déroulement. Il s'agit de pouvoir garantir que l'émission, la modification, la réception d'une information ne soient pas réfutées ou que toutes les actions réalisées sur un composant des Systèmes d'Information puissent être contrôlées et auditées.<br>La preuve recouvre trois notions complémentaires :<br>▪ la traçabilité : obtenir des traces décrivant la manipulation,<br>▪ l'imputabilité : pouvoir attribuer une action,<br>▪ la non-répudiation : impossibilité de nier une action. |
| **Tiers** | Le terme « Tiers » désigne l'ensemble des stagiaires, des prestataires, des fournisseurs, des partenaires et des travailleurs intérimaires employés à titre individuel par France Travail ; ces personnels sont amenés à travailler, de manière permanente ou occasionnelle, sur les Systèmes d'Information de France Travail et, de ce fait, à avoir accès à des informations ou à des ressources de France Travail.<br>. |



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

Diffusion interne

## 6.2. LISTE DES RÈGLES

TST-01 Définition des exigences de sécurité ..... 12
TST-02 Contractualisation des interventions des tiers ..... 12
TST-03 Engagement de confidentialité et respect des exigences de sécurité ..... 13
TST-04 Pilotage des interventions des tiers ..... 13
TST-05 Validation des accès du tiers au Système d'Information de France Travail ..... 13
TST-06 Inventaire des accès logiques et physiques ..... 13
TST-07 Traçabilité des accès logiques et physiques ..... 13
TST-08 Fin d'intervention du tiers ..... 14

(*Fin de document*)



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

Diffusion interne