

EXTERNALISATION DE DONNÉE

QUESTIONNAIRE SÉCURITÉ

Référence	SSI-QUE-TST_Externalisation de donnée - Questionnaire_V1.2
Clef GED	198667
Version	V1.3
Classification	Public
Date	13/06/2017
État	Validé
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	DGA-DMR

Identification du document		
Référence	Titre du document	
SSI-QUE-TST_Externalisation de donnée - Questionnaire_V1.2	Externalisation de donnée-Questionnaire SSI	
Version	État du document	Auteurs
1.3	Final	Filière Sécurité des SI

Classification	
Niveau	Diffusion
Public	Portée publique, diffusion sans restriction

Mises à jour		
Version	Date	Nature de la modification
1.0	24 Janvier 2014	Création du document
1.1	29 septembre 2014	Relecture thématique SSI – groupe de travail filière SSI
1.2	13 juin 2017	Mises à jour dans le cadre de la refonte du référentiel initiée en 2016
1.3	22 Janvier 2024	Mise a jour dans le cadre du changement de marque

Relectures et validations				
Version	Relu par	Direction	Date	Statut
1.0	RSSI Sylvain Lambert	DSI	30/06/2014	validé
1.1	RSSI Sylvain Lambert	DSI	29/09/2014	validé
1.2	RSSI Sylvain Lambert	DSI	13/06/2017	validé
1.2	Robert Laupy	DGA-DMR	29/06/2017	validé

Documents de référence	
Référence colibri	Titre du document

SOMMAIRE

1. OBJECTIF ET CONTENU.....	4
1.1 OBJECTIF DU DOCUMENT	4
1.2 CONTENU DU DOCUMENT.....	4
2. QUESTIONNAIRE SÉCURITÉ	5
POLITIQUE DE SÉCURITÉ DE L'INFORMATION ET GESTION DU RISQUE	5
ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION	6
SÉCURITÉ DES RESSOURCES HUMAINES	6
CONTRÔLE D'ACCÈS ET GESTION DES IDENTITÉS.....	6
SÉCURITÉ DES DONNÉES	8
SÉCURITÉ LIÉE À L'EXPLOITATION.....	9
SÉCURITÉ DES RÉSEAUX.....	11
CRYPTOGRAPHIE	12
SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE	13
DÉVELOPPEMENT SÉCURISÉ.....	14
RELATION AVEC LES TIERS.....	14
GESTION DES INCIDENTS ET CONTINUITÉ D'ACTIVITÉ.....	15
CONFORMITÉ.....	16
EXIGENCES SUPPLÉMENTAIRES.....	17

1. OBJECTIF ET CONTENU

1.1 OBJECTIF DU DOCUMENT

Ce document 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.

Dans le cadre de la mission qui est lui est confiée en tant qu'institution nationale publique, France Travail est soumis à une réglementation stricte concernant la protection des données dont elle a la charge et les traitements qu'elle doit assurer.

Lorsqu'une partie des informations que possède France Travail est externalisée hors de ses structures, France Travail attend du fournisseur de service à qui sont confiées ces informations, un engagement sur le niveau de sécurité du Système d'Information concerné.

- Ces fournisseurs de service doivent répondre aux exigences de sécurité de France Travail, en adoptant les mesures de sécurité nécessaires.
- De plus, ils sont tenus à respecter les contraintes légales et réglementaires, auxquelles est soumis France Travail.

Les réponses du soumissionnaire au questionnaire sécurité constituent un engagement formel. Les mesures décrites dans le questionnaire doivent pouvoir être auditées par France Travail.

1.2 CONTENU DU DOCUMENT

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.

Les critères de sécurité concernés sont mentionnés en regard de chaque question posée.

Critères de sécurité		Exemple de risques concernés
D	Disponibilité	Non continuité du service.
I	Intégrité	Altération ou perte des informations de France Travail dans le SI de l'hébergeur. Incohérence entre les données fournies par France Travail et celles utilisées/publiées par l'hébergeur sur son SI.
C	Confidentialité	Divulgence d'informations confidentielles à des personnes non autorisées.
P	Preuve	Incapacité à démontrer la responsabilité d'un tiers.

2. QUESTIONNAIRE SÉCURITÉ

Questions		Critères de sécurité	Réponses
Politique de sécurité de l'information et gestion des risques			
1	Appliquez-vous le guide d'hygiène informatique de l'ANSSI au SI hébergeant le service proposé ?	D, I, C, P	
2	Disposez-vous de la qualification « Prestataire de service d'informatique en nuage(SecNumCloud) » délivrée par l'ANSSI ? Si oui, de quel niveau s'agit-il : « Essentiel » ou « Avancé » ?	D, I, C, P	
3	Une politique de sécurité est-elle formalisée au sein de l'entreprise ? Identifie-t-elle les engagements du prestataire quant au respect de la législation et réglementation nationale en vigueur relative aux données confiées ?	D, I, C, P	
4	Quels référentiels ou normes sont appliqués pour la prise en compte de la sécurité sur le SI ?	D, I, C, P	
5	Une analyse de risques des systèmes d'informations est-elle réalisée en amont des projets pouvant avoir un impact sur le service utilisé par France Travail?	D, I, C, P	

Questions		Facteur de sécurité	Réponses
6	Une analyse de risques sur le périmètre du service utilisé par France Travail a-t-elle été réalisée ? Les risques résiduels identifiés ont-ils été formellement acceptés par la direction ?	D, I, C, P	
Organisation de la sécurité de l'information			
7	Comment est organisée la sécurité au sein de l'entreprise ? (rôles, responsabilités, séparation des tâches, etc.)	D, I, C, P	
Sécurité des ressources humaines			
8	Quels sont les engagements de confidentialité du personnel impliqué dans le service vis-à-vis des données de France Travail auxquelles ils ont accès?	C	
9	Quels sont les moyens mis en œuvre afin de sensibiliser le personnel à la sécurité de l'information ?	D, I, C	
Contrôle d'accès et gestion des identités			
10	Comment sont protégées les ressources contre les accès non autorisés ?	I, C, P	

Questions		Facteur de sécurité	Réponses
11	Dans le cas d'utilisation de mots de passe, comment sont protégés ces mots de passe ? Les règles et recommandations de l'ANSSI sont-elles appliquées?	I, C, P	
12	Comment sont mises en œuvre les habilitations des ayant droits France Travail (processus, validation, certification) ?	I, C, P	
13	Comment sont gérés (attribution, suppression, revue) les droits d'accès logiques des administrateurs et utilisateurs (employés, sous-traitants ou prestataires) ?	I, C, P	
14	Comment sont protégés et contrôlés les flux d'administrations (réseau dédié, chiffrement etc.) ?	I, C, P	
15	Comment sont tracés les accès aux données de France Travail et aux systèmes hébergeant ces données (accès des utilisateurs et des administrateurs) ?	P	
16	Les agents de France Travail bénéficient du SSO sur leur poste de travail. Comment appliquer ce mode d'authentification sur le service hébergé ?	C	

Questions		Facteur de sécurité	Réponses
Sécurité des données			
17	Par quels mécanismes les données sensibles de France Travail sont-elles isolées des autres données clients ?	C	
18	Quels sont les moyens d'assurer la protection des données pendant les traitements et le stockage (interdiction des supports amovibles, chiffrement éventuellement, ...) ?	D, C	
19	En cas de chiffrement de données, quels types de chiffrement sont utilisés ? Les règles et recommandations de l'ANSSI sont-elles appliquées ?	C	
20	Quels moyens assurent la protection des données sensibles sauvegardées ?	C	
21	Comment sont protégées les données de France Travail contre la divulgation par les intervenants (personnels, sous-traitants) ?	C	
22	Quels sont les moyens mis en œuvre pour détecter une perte ou un vol de données sensibles ou données personnelles ? Quelle est la procédure d'alerte auprès de France Travail ?	D, C	

Questions		Facteur de sécurité	Réponses
Sécurité liée à l'exploitation			
23	Quels processus sont mis en œuvre pour gérer les changements sur les systèmes et moyens de traitement de l'information ?	D, I	
24	Comment est assurée la séparation entre les environnements de développement, de test et d'exploitation ?	D, I	
25	Comment sont protégées les données de tests en pré-production ?	I, C	
26	Quelles mesures sont mises en œuvre pour lutter contre les codes malveillants? (détection, prévention, restauration, sensibilisation)	D, I, C, P	
27	Quelles est la politique de sauvegarde et l'organisation de la vérification du bon fonctionnement des sauvegardes ?	D	
28	Quels sont les moyens mis en œuvre pour assurer le suivi des événements de sécurité et la protection de l'information?	D, I, C	

Questions		Facteur de sécurité	Réponses
29	Un système de détection des incidents de sécurité est-il mis en place ?	D, I, C	
30	Les horloges de tous les dispositifs actifs du SI sont-elles synchronisées à une source de temps précise et préalablement définie afin de permettre un enregistrement exact et précis des événements ?	P	
31	Existe-t-il une organisation pour le maintien opérationnel des systèmes et logiciels utilisés par le service ? (alerte sur les vulnérabilités, gestion des patches...)	D, I, C	
32	Quels moyens sont mis en place pour se prémunir des incidents sur les environnements de production, dues à des erreurs d'exploitation ou des erreurs d'environnement de qualification le cas échéant ?	D, I, C	
33	Quels moyens sont mis en place pour éviter un dépassement des limites du matériel ou des logiciels supportant le service ?	D	

Questions		Facteur de sécurité	Réponses
Sécurité des réseaux			
34	Existe-t-il une cartographie du SI relatif au service ? (ressources matérielles/physiques, schéma d'architecture, matrice des flux réseaux, etc.)	D, I	
35	Quelles sont les mesures de cloisonnement mises en œuvre pour séparer les flux réseaux (selon la sensibilité des informations, la nature du flux, le type de client, etc.)	D, C	
36	Quels moyens sont mis en place pour éviter une saturation, une dégradation ou une indisponibilité de la liaison télécom vers France Travail ou les usagers du service hébergé ?	D	
37	Quels sont les dispositifs mis en place pour détecter et prévenir les intrusions ?	D, I, P	
38	Comment est protégé le réseau contre les attaques ciblées (Déni de service distribué, spoofing) ?	D, I, C	

Questions		Facteur de sécurité	Réponses
Cryptographie			
39	Si des mécanismes de chiffrement des flux réseaux sont mis en œuvre, les règles et recommandations de l'ANSSI sont-elles appliquées ?	I, C	
40	Si un mécanisme de signature électronique est mis en œuvre, les règles et recommandations de l'ANSSI sont-elles appliquées ?	P	
41	Si des clés cryptographiques sont mises en œuvre, comment l'accès à ces clefs est-il protégé ? Les règles et recommandations de l'ANSSI sont-elles appliquées ?	C	

Questions		Facteur de sécurité	Réponses
Sécurité physique et environnementale			
42	Quels sont les moyens de protection des accès physiques aux sites / zones ?	D, I, C	
43	Quelles protections sont mises en œuvre pour se protéger du vol, de la détérioration ou de la perte de matériel contenant des données sensibles ?	D, I, C	
44	Comment sont gérés (attribution, suppression, revue) les droits d'accès physiques des intervenants (employés, sous-traitants ou prestataires) ?	D, I, C	
45	Quels moyens sont mis en œuvre pour protéger les sites /zones des menaces extérieures et environnementales ? (incendie, dégât des eaux, risques climatiques, inondations, séismes, etc.)	D	
46	Quels moyens sont mis en œuvre pour protéger le câblage électrique et de télécommunication des dommages physiques et des possibilités d'interception ?	D, C	
47	Comment sont gérés la maintenance, la réutilisation, le remplacement et la destruction des matériels ?	I, C	

Questions		Facteur de sécurité	Réponses
48	Quels moyens assurent la suppression des données sensibles des supports en cas de mise au rebut ou en cas de réparation ?	C	
Développement sécurisé			
49	Existe-t-il une politique définissant des règles de développement sécurisé afin de créer des services ou applications sécurisés ? Quels moyens sont mis en œuvre afin d'intégrer la sécurité dans le développement des logiciels/applications/services ?	D, I, C	
50	Des tests de sécurité et de conformité sont-ils réalisés durant la phase de développement ?	I, C	
Relation avec les tiers			
51	Existe-t-il une liste répertoriant l'ensemble des tiers qui participent à la mise en œuvre du service ? (hébergeur, développeur, sous-traitant, etc.)	C	
52	Comment est déployée la politique de sécurité auprès de ces tiers ?	D, I, C, P	

53	Quels processus sont mis en œuvre pour assurer le suivi des changements apportés par les tiers susceptibles d'affecter le niveau de sécurité du service ?	D, I, C	
54	Faites-vous signer un engagement de confidentialité aux tiers participant à la mise en œuvre du service vis-à-vis des données de France Travail auxquelles ils ont accès ?	C	
Questions		Facteur de sécurité	Réponses
Gestion des incidents et continuité d'activité			
55	Quels processus sont mis en œuvre pour gérer les incidents liés à la sécurité de l'information ? (rôles/responsabilité, détection, réponse, capitalisation, communication, etc.) ?	D, I, C	
56	Comment est assurée la continuité de service en cas d'incident technique (panne électrique, climatisation) ou d'incident de sécurité ?	D	
57	Quels sont les processus de mise en œuvre, vérification, revue et évaluation du plan de continuité d'activité (en cas de perte informatique, indisponibilité humaine etc.) ?	D	
58	En cas de fermeture ou d'acquisition par un tiers, comment assurez-vous la continuité du service ?	D, I, C	

Questions		Facteur de sécurité	Réponses
Conformité			
59	Quels processus sont mis en œuvre afin d'assurer le respect des exigences légales, réglementaires et contractuelles en vigueur applicables au service utilisé par France Travail ?	C , P	
60	Des audits externes sont-ils réalisés régulièrement sur le périmètre du service utilisé par France Travail ? (audit de configuration, test d'intrusion, audit de code source)	D, I, C, P	
61	Quels contrôles sont mis en place pour s'assurer du respect des politiques et normes de sécurité ?	D, I, C, P	

Questions		Facteur de sécurité	Réponses
Exigences supplémentaires			
62	Quels sont les moyens et l'organisation mis en place pour assurer la réversibilité en cas de fin de prestation de service ?	D, I, C	
63	Où seront localisées les données de France Travail ? Depuis quels lieux, les opérations de maintenance et de supervision du service, utilisé par France Travail, seront réalisées ?	C, P	
64	Comment sont garanties la restitution des données à France Travail, l'intégrité et l'intégralité des données, ainsi que la suppression sur les infrastructures du service de Cloud ?	D, I, C, P	
65	En fonction du type et de la sensibilité des données, comment est gérée la durée de rétention dans vos systèmes de sauvegarde ? A la fin de cette durée, quels sont les moyens mis en place pour assurer une destruction effective des données ?	C	