HEBERGEMENT SERVICES EN LIGNE OU CLOUD

RÈGLES DE SÉCURITÉ

Référence	SSI-REG-TST_Hébergement Services en Ligne ou Cloud_V1.1
Clef GED	273304
Version	V1.1
Classification	Interne
Date	15/05/2018
État	Validé
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	Direction de la maîtrise des risques

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

Identification du document

Référence	Titre du document	
SSI-REG-TST_Hébergement Services en Ligne ou Cloud_V1.1	Hébergement Services en ligne ou Cloud	
Version	**État du document**	**Auteurs**
1.1	Final	Filière Sécurité des SI

Classification

Niveau	Diffusion
Interne	Le personnel de Pôle emploi 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	23 mars 2017	Création du document
1.0	04/05/2017	Finalisation du document
1.1	15/05/2018	Modification apportée dans le titre du document et dans le paragraphe « Objet du document » pour accentuer le fait que ce document s'applique à de l'hébergement de services accédés en ligne ou de données en CLOUD.

Relectures et validations

Version	Relu par	Direction	Date	Statut
1.0	RSSI Sylvain Lambert	DSI	04/05/2017	Validé
1.0	Robert Laupy	DGA-DMR	29/06/2017	Validé
1.1	RSSI Sylvain Lambert	DSI	15/05/2018	Validé
1.1	Mojdeh Hodjat-Panah-Daurelle	DMRS		

Documents de référence

Référence colibri	Titre du document

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

SOMMAIRE

1. Objet du document 5
2. Règles de sécurité 6
2.1. Politique de sécurité de l'information et gestion du risque 6
2.2. Organisation de la sécurité de l'information 7
2.3. Sécurité des ressources humaines 8
2.4. Gestion des actifs 9
2.5. Contrôle d'accès et gestion des identités 10
2.6. Sécurité des données 13
2.7. Sécurité liée à l'exploitation 14
2.8. Sécurité des réseaux 17
2.9. Cryptographie 18
2.10. Sécurité physique et environnementale 19
2.11. Acquisition, développement et maintenance des systèmes d'information 21
2.12. Relation avec les tiers 23
2.13. Gestion des incidents et continuité d'activité 24
2.14. Conformité 26
2.15. Exigences supplémentaires 27
3. Annexe 28
3.1. Listes des règles 28

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

Règles typographiques

Les règles de la thématique « hébergement de Services en ligne ou Cloud » sont préfixées par le sigle « **CLD**- » 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.

1. OBJET DU DOCUMENT

Ce document regroupe l'ensemble des exigences de sécurité applicables à un prestataire hébergeant un service de Pole emploi accessible en ligne, ci-après dénommé le « prestataire » et/ou partenaire.

Il permet à Pôle Emploi de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité de sa prestation et sur la confiance que Pôle Emploi peut lui accorder.

Ce document s'applique également dans les cas de services hébergés en Cloud tels que :

- Services SaaS : mise à disposition par le prestataire d'applications hébergées sur une plateforme Cloud ;
- Service PaaS : mise à disposition par le prestataire de plateformes d'hébergement d'applications ;
- Service IaaS : mise à disposition par le prestataire de ressources informatiques abstraites (puissance CPU, mémoire, stockage, etc.)

Ces exigences de sécurité sont applicables :

- Aux procédures de mise en concurrence pour des services hébergés à l'extérieur de Pôle emploi ;
- Aux contrats ou conventions liant un prestataire ou partenaire à Pôle Emploi.

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).

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2. REGLES DE SECURITE

2.1. POLITIQUE DE SÉCURITÉ DE L'INFORMATION ET GESTION DU RISQUE

CLD- 01 Guide d'hygiène de l'ANSSI

- Le prestataire applique au service les règles de sécurité préconisées par le guide d'hygiène informatique de l'ANSSI.

CLD- 02 Politique de sécurité de l'information

- Le prestataire documente et met en œuvre une politique de sécurité de l'information relative au service.
- La politique de sécurité de l'information doit identifier les engagements du prestataire quant au respect de la législation et réglementation nationale en vigueur selon la nature des informations qui pourraient être confiées par Pôle Emploi au prestataire.
- La direction du prestataire doit approuver formellement la politique de sécurité de l'information.
- Le prestataire révise régulièrement sa politique de sécurité de l'information afin de prendre en compte l'évolution des menaces et les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

CLD- 03 Analyse de risques

- Le prestataire réalise et documente une analyse des risques couvrant l'ensemble du périmètre du service.
- Le prestataire réalise son appréciation de risques en utilisant une méthode documentée garantissant une démarche reproductible et des résultats comparables entre les différentes analyses.
- La direction du prestataire doit accepter formellement les risques résiduels identifiés dans l'analyse des risques.
- Le prestataire révise régulièrement l'appréciation des risques afin de prendre en compte l'évolution des menaces et les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.2. ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION

CLD- 04 Fonctions et responsabilités liées à la sécurité de l'information

- Le prestataire documente et met en œuvre une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l'information au sein de son organisation.
- Le prestataire désigne un responsable de la sécurité des systèmes d'information

CLD- 05 Relation avec les autorités

- Le prestataire met en place des relations appropriées avec les autorités compétentes en matière de sécurité de l'information et des données à caractère personnel et, le cas échéant, avec les autorités sectorielles selon la nature des informations confiées par Pôle Emploi.

CLD- 06 Relation avec les groupes de travail spécialisés

- Le prestataire entretient des contacts appropriés avec des groupes de spécialistes ou des sources reconnues, notamment pour prendre en compte de nouvelles menaces et les mesures de sécurité appropriées pour les contrer.

CLD- 07 La sécurité de l'information dans la gestion de projet

- Le prestataire réalise et documente une analyse de risques préalablement à tout projet pouvant avoir un impact sur le service, quelle que soit la nature du projet.
- Dans la mesure où un projet affecte ou est susceptible d'affecter le niveau de sécurité du service, le prestataire avertit Pôle Emploi des impacts potentiels, des mesures mises en place pour réduire ces impacts ainsi que des risques résiduels le concernant.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.3. SÉCURITÉ DES RESSOURCES HUMAINES

CLD- 08 Rupture, terme ou modification du contrat de travail

- Le prestataire définit et attribue les rôles et les responsabilités relatives à la rupture, au terme ou à la modification de tout contrat avec une personne impliquée dans la fourniture du service.

CLD- 09 Sensibilisation et formation à la sécurité de l'information

- Le prestataire sensibilise à la sécurité de l'information l'ensemble des personnes impliquées dans la fourniture du service.
- Le prestataire documente et met en œuvre un plan de formation concernant la sécurité de l'information adapté au service et aux missions des personnels.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.4. GESTION DES ACTIFS

CLD- 10 Propriété des actifs

- Le prestataire s'assure de la validité des licences des logiciels tout au long de la prestation.

CLD- 11 Identification des besoins de sécurité de l'information

- Le prestataire identifie les différents besoins de sécurité des informations relatives au service.

CLD- 12 Marquage et manipulation de l'information

- Le prestataire documente et met en œuvre une procédure pour le marquage et la manipulation de toutes les informations participant à la délivrance du service, conformément à son besoin de sécurité.

CLD- 13 Gestion des supports amovibles

- Le prestataire documente et met en œuvre une procédure pour la gestion des supports amovibles.
- Les supports amovibles utilisés sur l'infrastructure technique ou pour des tâches d'administration doivent être dédiés à un usage.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.5. CONTRÔLE D'ACCÈS ET GESTION DES IDENTITÉS

CLD- 14 Enregistrement et désinscription des utilisateurs

- Le prestataire documente et met en œuvre une procédure d'enregistrement et de désinscription des utilisateurs s'appuyant sur une interface de gestion des comptes et des droits d'accès. Cette procédure doit indiquer quelles données doivent être supprimées au départ d'un utilisateur.
- Le prestataire attribue des comptes nominatifs lors de l'enregistrement des utilisateurs placés sous sa responsabilité.
- Le prestataire met en œuvre des moyens permettant de s'assurer que la désinscription d'un utilisateur entraîne la suppression de tous ses accès aux ressources du service ainsi que la suppression de ses données.

CLD- 15 Politiques et contrôle d'accès

- Le prestataire documente et met en œuvre une politique de contrôle d'accès.
- Le prestataire révise annuellement la politique de contrôle d'accès et à chaque changement majeur pouvant avoir un impact sur le service.

CLD- 16 Gestion des droits d'accès

- Le prestataire documente et met en œuvre une procédure permettant d'assurer l'attribution, la modification et le retrait de droits d'accès aux ressources du système d'information du service.
- Le prestataire met à la disposition de Pôle Emploi les outils et les moyens permettant une différenciation des rôles des utilisateurs du service, par exemple suivant leur rôle fonctionnel.
- Le prestataire tient à jour l'inventaire des utilisateurs sous sa responsabilité disposant de droits d'administration sur les ressources du service.
- Le prestataire inclut dans la procédure de gestion des droits d'accès les actions de révocation ou de suspension des droits de tout utilisateur.

CLD- 17 Revue des droits d'accès utilisateurs

- Le prestataire révise annuellement les droits d'accès des utilisateurs sur son périmètre de responsabilité.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

CLD- 18 Gestion des authentifications des utilisateurs

- Le prestataire formalise et met en œuvre des procédures de gestion de l'authentification des utilisateurs.
- Tout mécanisme d'authentification doit prévoir le blocage d'un compte après un nombre limité de tentatives infructueuses.
- Lorsque des comptes techniques, non nominatifs, sont nécessaires, le prestataire met en place des mesures obligeant les utilisateurs à s'authentifier avec leur compte nominatif avant de pouvoir accéder à ces comptes techniques.

CLD- 19 Accès aux interfaces d'administration

- Les comptes d'administration sous la responsabilité du prestataire doivent être gérés à l'aide d'outils et d'annuaires distincts de ceux utilisés pour la gestion des comptes utilisateurs placés sous la responsabilité de Pôle Emploi.
- Les interfaces d'administration mises à disposition de Pôle Emploi doivent être distinctes des interfaces d'administration utilisées par le prestataire.
- Les interfaces d'administration utilisées par le prestataire ne doivent pas être accessibles à partir d'un réseau public et ainsi ne doivent permettre aucune connexion des utilisateurs sous la responsabilité de Pôle Emploi.
- Si des interfaces d'administration sont mises à disposition de Pôle Emploi avec un accès via un réseau public, les flux d'administration doivent être authentifiés et chiffrés.
- Le prestataire met en place un système d'authentification à double facteur pour l'accès:
  - aux interfaces d'administration utilisées par le prestataire ;
  - aux interfaces d'administration dédiées à Pôle Emploi.
- Si des interfaces d'administration sont mises à disposition de Pôle Emploi avec un accès via un réseau public, les flux d'administration doivent être authentifiés et chiffrés.
- Dès lors qu'une interface d'administration est accessible depuis un réseau public, le processus d'authentification doit avoir lieu avant toute interaction entre l'utilisateur et l'interface en question.
- Dans le cadre d'un service SaaS, les interfaces d'administration mises à disposition des clients doivent être différenciées des interfaces permettant l'accès des utilisateurs finaux.
- Lorsque le prestataire utilise un service de type IaaS comme socle d'un autre type de service (PaaS ou SaaS), les ressources affectées à l'usage du prestataire ne doivent en aucun cas être accessibles via l'interface publique mise à disposition des autres clients du service IaaS.
- Lorsque le prestataire utilise un service de type PaaS comme socle d'un autre type de service (typiquement SaaS), les ressources affectées à l'usage du prestataire ne doivent en aucun cas être accessibles via l'interface publique mise à disposition des autres clients du service PaaS.

CLD- 20 Restriction des accès à l'information

- Le prestataire met en œuvre des mesures de cloisonnement appropriées entre ses clients.
- Le prestataire met en œuvre des mesures de cloisonnement appropriées entre le service et ses autres systèmes d'information (bureautique, informatique de gestion, gestion technique du bâtiment, contrôle d'accès physique, etc.).
- Le prestataire doit concevoir, développer, configurer et déployer le service en assurant au moins un cloisonnement entre l'infrastructure technique et les équipements nécessaires à l'administration des services et des ressources qu'elle héberge.

2.6. SÉCURITÉ DES DONNÉES

CLD- 21 Chiffrement des données stockées

- Le prestataire définit et met en œuvre un mécanisme de chiffrement empêchant la récupération des données de Pôle Emploi en cas de réallocation d'une ressource ou de récupération du support physique.
- Les méthodes de chiffrement utilisées doivent respecter les règles et recommandations de l'ANSSI.

CLD- 22 Procédure d'alerte

- Le prestataire définit et met en œuvre une procédure d'alerte permettant d'informer Pôle Emploi en cas de vol, divulgation ou perte de ses données.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.7. SÉCURITÉ LIÉE À L'EXPLOITATION

CLD- 23 Procédures d'exploitation documentées

- Le prestataire documente les procédures d'exploitation, les tient à jour et les rend accessibles au personnel concerné.

CLD- 24 Gestion des changements

- Le prestataire documente et met en œuvre une procédure de gestion des changements apportés aux systèmes et moyens de traitement de l'information.
- Dans le cadre d'un service PaaS, le prestataire informe au plus tôt Pôle Emploi de toute modification à venir sur des éléments logiciels sous sa responsabilité dès lors que la compatibilité complète ne peut être assurée.
- Dans le cadre d'un service SaaS, le prestataire informer au plus tôt Pôle Emploi de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour Pôle Emploi.

CLD- 25 Séparation des environnements de développement, de test et d'exploitation

- Le prestataire doit documenter et mettre en œuvre les mesures permettant de séparer physiquement les environnements liés à la production du service des autres environnements, dont les environnements de développement.

CLD- 26 Sauvegarde des informations

- Le prestataire documente et met en œuvre une politique de sauvegarde et de restauration des données sous sa responsabilité dans le cadre du service.
- Le prestataire documente et met en œuvre des mesures de protection des sauvegardes.
- Le prestataire documente et met en œuvre une procédure permettant de tester régulièrement la restauration des sauvegardes.
- Le prestataire doit localiser les sauvegardes à une distance suffisante des équipements principaux en cohérence avec les résultats de l'analyse de risques et permettant de faire face à des sinistres majeurs.

CLD- 27 Mesures contre les codes malveillants

- Le prestataire documente et met en œuvre les mesures de détection, de prévention et de restauration pour se protéger des codes malveillants.
- Le prestataire documente et met en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l'impact d'une infection.

CLD- 28 Journalisation des événements

- Le prestataire documente et met en œuvre une politique de journalisation.
- Le prestataire génère et collecte les événements suivants : les activités des utilisateurs liées à la sécurité de l'information, la modification des droits d'accès, les événements issus des mécanismes de lutte contre les codes malveillants, les exceptions, les défaillances et tout autre événement lié à la sécurité de l'information.
- Le prestataire conserve les événements issus de la journalisation pendant une durée minimale de douze mois glissant sous réserve du respect des exigences légales et réglementaires.
- Le prestataire fournit, sur demande de Pôle Emploi, l'ensemble des événements le concernant.

CLD- 29 Protection de l'information journalisée

- Le prestataire protège les équipements de journalisation et les événements journalisés contre les atteintes à leur disponibilité, intégrité ou confidentialité.
- Le prestataire gère le dimensionnement de l'espace de stockage de l'ensemble des équipements hébergeant une ou plusieurs sources de collecte afin de permettre la conservation locale des événements journalisés prévue par la politique de journalisation des événements.
- Le prestataire met en place une sauvegarde des événements collectés suivant une politique adaptée.
- Le prestataire exécute les processus de journalisation et de collecte des évènements avec des comptes disposant de privilèges nécessaires et suffisants et limite l'accès aux événements journalisés.

CLD- 30 Synchronisation des horloges

- Le prestataire documente et met en œuvre une synchronisation des horloges de l'ensemble des équipements sur une ou plusieurs sources de temps internes cohérentes entre elles. Ces sources pourront elles-mêmes être synchronisées sur plusieurs sources fiables externes, sauf pour les réseaux isolés.
- Le prestataire doit mettre en place l'horodatage de chaque événement journalisé.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

CLD- 31 Analyse et corrélation des événements

- Le prestataire documente et met en œuvre une infrastructure permettant l'analyse et la corrélation des événements enregistrés par le système de journalisation afin de détecter les événements susceptibles d'affecter la sécurité du système d'information du service, en temps réel ou a posteriori pour des événements remontant jusqu'à douze mois.

CLD- 32 Installation de logiciels sur des systèmes en exploitation

- Le prestataire documente et met en œuvre une procédure permettant de contrôler l'installation de logiciels sur les équipements du système d'information du service.
- Le prestataire documente et met en œuvre une procédure de gestion de la configuration des environnements logiciels mis à la disposition de Pôle Emploi, notamment pour leur maintien en condition de sécurité.

CLD- 33 Gestion des vulnérabilités techniques

- Le prestataire documente et met en œuvre un processus de veille permettant de gérer les vulnérabilités techniques des logiciels et des systèmes utilisés dans le système d'information.

CLD- 34 Administration

- Le prestataire documente et met en œuvre une procédure obligeant les administrateurs sous sa responsabilité à utiliser des terminaux dédiés pour la réalisation exclusive des tâches d'administration. Il doit les maîtriser et les maintenir à jour.
- Le prestataire met en place des mesures de durcissement de la configuration des terminaux utilisés pour les tâches d'administration.
- Lorsque le prestataire autorise une situation de mobilité pour les administrateurs sous sa responsabilité, il doit l'encadrer par une politique documentée. La solution mise en œuvre doit notamment inclure :
  - l'utilisation d'un tunnel chiffré, non débrayable et non contournable, pour l'ensemble des flux;
  - le chiffrement intégral du disque.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.8. SÉCURITÉ DES RÉSEAUX

CLD- 35 Cartographie du système d'information.

- Le prestataire établi et tient à jour une cartographie du système d'information. Il révise au moins annuellement la cartographie.

CLD- 36 Cloisonnement des réseaux

- Le prestataire documente et met en œuvre les mesures de cloisonnement (logique, physique ou par chiffrement) pour séparer les flux réseau selon :
  - la sensibilité des informations transmises ;
  - la nature des flux (production, administration, supervision, etc.) ;
  - le domaine d'appartenance des flux (des clients – avec distinction par client ou ensemble de clients, du prestataire, des tiers, etc.) ;
  - le domaine technique (traitement, stockage, etc.).
- Le prestataire cloisonne, physiquement ou par chiffrement, tous les flux de données internes au service vis-à-vis de tout autre système d'information.
- Dans le cas où le réseau d'administration de l'infrastructure technique ne fait pas l'objet d'un cloisonnement physique, les flux d'administration doivent transiter dans un tunnel chiffré.
- Le prestataire met en place et configure un pare-feu applicatif pour protéger les interfaces d'administration destinées à Pôle Emploi et exposées sur un réseau public.
- Le prestataire doit mettre en œuvre sur l'ensemble des interfaces d'administration et de supervision de l'infrastructure technique du service un mécanisme de filtrage n'autorisant que les connexions légitimes identifiées dans la matrice des flux autorisés.

CLD- 37 Surveillance des réseaux

- Le prestataire doit disposer d'une ou plusieurs sondes de détection d'incidents de sécurité sur le service.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.9. CRYPTOGRAPHIE

CLD- 38 Chiffrement des flux

- Le prestataire respecte les règles et recommandations de l'ANSSI dans la mise en œuvre d'un mécanisme de chiffrement des flux réseau.

CLD- 39 Non répudiation

- Le prestataire respecte les règles et recommandations de l'ANSSI dans la mise en œuvre d'un mécanisme de signature électronique.

CLD- 40 Gestion des secrets

- Le prestataire met en œuvre des clés cryptographiques respectant les règles et recommandations de l'ANSSI.
- Le prestataire protège l'accès aux clés cryptographiques et autres secrets utilisés pour le chiffrement des données par un moyen adapté : conteneur de sécurité (logiciel ou matériel) ou support disjoint.
- Le prestataire protège l'accès aux clés cryptographiques et autres secrets utilisés pour les tâches d'administration par un conteneur de sécurité adapté, logiciel ou matériel.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.10. SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

CLD- 41 Périmètres de sécurité physique

- Le prestataire documente et met en œuvre des périmètres de sécurité, incluant le marquage des zones et les différents moyens de limitation et de contrôle des accès.

Commentaires

Le prestataire peut distinguer des zones publiques, des zones privées et des zones sensibles :

- Zones publiques : elles sont accessibles à tous dans les limites de la propriété du prestataire. Le prestataire ne doit héberger aucune ressource dévolue au service ou permettant d'accéder à des composantes de celui-ci dans les zones publiques.
- Zones privées : elles peuvent héberger les plateformes et moyens de développement du service, les postes d'administration, d'exploitation et de supervision, les locaux à partir desquels le prestataire opère.
- Zones sensibles elles sont réservées à l'hébergement du système d'information de production du service hors postes d'administration, d'exploitation et de supervision.

CLD- 42 Contrôle d'accès physique

- Le prestataire doit protéger les zones non publiques contre les accès non autorisés. il doit mettre en œuvre un contrôle d'accès physique reposant sur un ou deux facteurs personnels (suivant la sensibilité de la zone).
- Le prestataire documente et met en œuvre les moyens permettant de s'assurer que les visiteurs sont systématiquement accompagnés par le prestataire lors de leurs accès et séjours en zones non publiques. Le prestataire conserve une trace de l'identité des visiteurs conformément à la législation et réglementation en vigueur.
- Le prestataire documente et met en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones non publiques.
- Le prestataire met en place une journalisation des accès physiques aux zones non publiques. Il doit effectuer une revue régulière de ces journaux.

CLD- 43 Protection contre les menaces extérieures et environnementales

- Le prestataire documente et met en œuvre les moyens permettant de minimiser les risques inhérents aux sinistres physiques (incendie, dégât des eaux, etc.) et naturels (risques climatiques, inondations, séismes, etc.).
- Le prestataire documente et met en œuvre les mesures permettant de prévenir et limiter les conséquences d'une coupure d'alimentation électrique et permettre une reprise du service conforme aux exigences de disponibilité du service établies avec Pôle Emploi.
- Le prestataire documente et met en œuvre les moyens permettant de maintenir des conditions de température et d'humidité adaptées aux équipements. De plus, il doit

mettre en œuvre des mesures permettant de prévenir les pannes de climatisation et d'en limiter les conséquences.

- Le prestataire documente et met en œuvre des contrôles et tests réguliers des équipements de détection et de protection physique.

CLD- 44 Sécurité du câblage

- Le prestataire documente et met en œuvre des mesures permettant de protéger le câblage électrique et de télécommunication des dommages physiques et des possibilités d'interception.
- Le prestataire doit établir et tenir à jour un plan de câblage.

CLD- 45 Maintenance des matériels

- Le prestataire documente et met en œuvre des mesures permettant de s'assurer que les conditions d'installation, de maintenance et d'entretien des équipements du système d'information du service sont compatibles avec les exigences de confidentialité et de disponibilité du service établies avec Pôle Emploi.
- Le prestataire doit souscrire des contrats de maintenance permettant de disposer des mises à jour de sécurité des logiciels installés sur les équipements du service.
- Le prestataire s'assure que les supports ne peuvent être retournés à un tiers que si les données de Pôle Emploi y sont stockées chiffrées ou ont préalablement été détruites à l'aide d'un mécanisme d'effacement sécurisé par réécriture de motifs aléatoires.

CLD- 46 Sortie des actifs Pôle emploi

- En cas de transfert hors site des données Pôle Emploi, le prestataire documente la procédure.
- Il informe Pôle emploi du transfert de ses données. Pôle emploi se réserve le droit de refuser par décision motivée.
- Le prestataire doit mettre en œuvre les moyens permettant de garantir que le niveau de protection en confidentialité et en intégrité des actifs durant leur transport est équivalent à celui sur site.

CLD- 47 Recyclage sécurisé du matériel

- Le prestataire documente et met en œuvre des moyens permettant d'effacer de manière sécurisée par réécriture de motifs aléatoires tout support de données mis à disposition d'un client.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.11. ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES D'INFORMATION

CLD- 48 Politique de développement sécurisé

- Le prestataire documente et met en œuvre des règles de développement sécurisé des logiciels et des systèmes, et les applique aux développements internes.
- Le prestataire documenter et met en œuvre une formation adaptée en développement sécurisé aux employés concernés.

CLD- 49 Procédures de contrôle des changements de système

- Le prestataire documente et met en œuvre une procédure de contrôle des changements apportés au système d'information du service.
- Le prestataire documente et met en œuvre une procédure de validation des changements apportés au système d'information du service sur un environnement de pré-production avant leur mise en production.
- Le prestataire conserve un historique des versions des logiciels et des systèmes mis en œuvre pour permettre de reconstituer, le cas échéant dans un environnement de test, un environnement complet tel qu'il était mis en œuvre à une date donnée.

CLD- 50 Revue technique des applications après changement en production

- Le prestataire documente et met en œuvre une procédure permettant de tester, préalablement à leur mise en production, l'ensemble des applications afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité du service.

CLD- 51 Environnement de développement sécurisé

- Le prestataire met en œuvre un environnement sécurisé de développement permettant de gérer l'intégralité du cycle de développement du système d'information du service.

CLD- 52 Développement externalisé

- Le prestataire document et met en œuvre une procédure permettant de superviser et de contrôler l'activité de développement externalisé des logiciels et systèmes.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

CLD- 53 Test de la sécurité et conformité du système

- Le prestataire soumet les systèmes d'information, nouveaux ou mis à jour, à des tests de conformité.

CLD- 54 Protection des données de test

- Le prestataire documente et met en œuvre une procédure permettant d'assurer l'intégrité des données de tests utilisés en pré-production.
- Si le prestataire souhaite utiliser des données Pôle Emploi issues de la production pour réaliser des tests, le prestataire doit préalablement obtenir l'accord de Pôle Emploi et les anonymiser. Le prestataire assure la confidentialité des données lors de leur anonymisation.

2.12. RELATION AVEC LES TIERS

CLD- 55 Identification des tiers

- Le prestataire tient à jour une liste de l'ensemble des tiers participant à la mise en œuvre du service (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance, fournisseurs de climatisation, etc.). Cette liste doit être exhaustive, préciser la contribution du tiers au service et tenir compte des cas de sous-traitance à plusieurs niveaux.

CLD- 56 La sécurité dans les accords conclus avec les tiers

- Le prestataire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des conventions, contrats ou accords à conclure. Le prestataire inclut ces exigences dans les contrats conclus avec les tiers.

CLD- 57 Surveillance et revue des services des tiers

- Le prestataire documente et met en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service.

CLD- 58 Gestion des changements apportés dans les services des tiers

- Le prestataire documente et met en œuvre une procédure de suivi des changements apportés par les tiers participant à la mise en œuvre du service susceptibles d'affecter le niveau de sécurité du système d'information du service.
- Dans la mesure où un changement de tiers participant à la mise en œuvre du service affecte le niveau de sécurité du service, le prestataire informe Pôle Emploi sans délais et met en œuvre les mesures permettant de rétablir le niveau de sécurité précédent.

CLD- 59 Engagements de confidentialité

- Le prestataire documente et met en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgation vis-à-vis des tiers participant à la mise en œuvre du service.

2.13. GESTION DES INCIDENTS ET CONTINUITÉ D'ACTIVITÉ

CLD- 60 Responsabilités et procédures

- Le prestataire documente et met en œuvre une procédure permettant d'apporter des réponses rapides et efficaces aux incidents de sécurité.
- Le prestataire informe ses employés et l'ensemble des tiers participant à la mise en œuvre du service de cette procédure.

CLD- 61 Signalements liés à la sécurité de l'information

- Le prestataire documente et met en œuvre une procédure exigeant de ses employés et des tiers participant à la mise en œuvre du service qu'ils lui rendent compte de tout incident de sécurité, avéré ou suspecté ainsi que de toute faille de sécurité.
- Le prestataire communique à Pôle Emploi les incidents de sécurité dans un délai maximum de 24 heures ainsi que les préconisations associées pour en limiter les impacts.
- Le prestataire communique les incidents de sécurité aux autorités compétentes conformément aux exigences légales et réglementaires en vigueur.

CLD- 62 Appréciation des événements liés à la sécurité de l'information et prise de décision

- Le prestataire doit apprécier les événements liés à la sécurité de l'information et décider s'il faut les qualifier en incidents de sécurité. Pour l'appréciation, il s'appuie sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec Pôle Emploi.

CLD- 63 Réponse aux incidents liés à la sécurité de l'information

- Le prestataire traite les incidents de sécurité jusqu'à leur résolution et doit en informer Pôle Emploi.
- Le prestataire archive les documents détaillant les incidents de sécurité.

CLD- 64 Tirer des enseignements des incidents liés à la sécurité de l'information

- Le prestataire documente et met en œuvre un processus d'amélioration continue afin de diminuer l'occurrence et l'impact de types d'incidents de sécurité déjà traités.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

CLD- 65 Recueil de preuves

- Le prestataire documente et met en œuvre une procédure permettant d'enregistrer les informations relatives aux incidents de sécurité et pouvant servir d'éléments de preuve.

CLD- 66 Organisation de la continuité d'activité

- Le prestataire doit documenter et mettre œuvre un plan de continuité d'activité prenant en compte la sécurité de l'information.
- Le prestataire doit réviser annuellement le plan de continuité d'activité du service et à chaque changement majeur pouvant avoir un impact le service.

CLD- 67 Mise en œuvre de la continuité d'activité

- Le prestataire documente et met en œuvre des procédures permettant de maintenir ou de restaurer l'exploitation du service et d'assurer la disponibilité des informations au niveau et dans les délais pour lesquels le prestataire s'est engagé vis-à-vis de Pôle Emploi.

CLD- 68 Vérifier, revoir et évaluer la continuité d'activité

- Le prestataire documente et met en œuvre une procédure permettant de tester le plan de continuité d'activités afin de s'assurer qu'il est pertinent et efficace en situation de crise.

CLD- 69 Disponibilité des moyens de traitement de l'information

- Le prestataire documente et met en œuvre les mesures qui lui permettent de répondre au besoin de disponibilité du service défini par Pôle Emploi.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.14. CONFORMITÉ

CLD- 70 Identification de la législation et des exigences contractuelles applicables

- Le prestataire identifie les exigences légales, réglementaires et contractuelles en vigueur applicables au service.
- Le prestataire documente et met en œuvre les procédures permettant de respecter les exigences légales, réglementaires et contractuelles en vigueur applicables au service, ainsi que les besoins de sécurité spécifiques.

CLD- 71 Revue indépendante de la sécurité de l'information

- Le prestataire documente et met en œuvre un programme d'audit définissant le périmètre et la fréquence des audits en accord avec la gestion du changement, les politiques, et les résultats de l'appréciation des risques.

CLD- 72 Conformité avec les politiques et les normes de sécurité

- Le prestataire via le responsable de la sécurité de l'information s'assure régulièrement de l'exécution correcte de l'ensemble des procédures de sécurité placées sous sa responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

2.15. EXIGENCES SUPPLÉMENTAIRES

CLD- 73 Réversibilité

- Le prestataire met en œuvre un mécanisme de réversibilité permettant à Pôle Emploi de récupérer l'ensemble de ses données (fournies directement par Pôle Emploi ou produites dans le cadre du service à partir des données ou des actions de Pôle Emploi).
- Le prestataire doit assurer cette réversibilité via l'une des modalités techniques suivantes :
  - la mise à disposition de fichiers suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni par le prestataire ;
  - la mise en place d'interfaces techniques permettant l'accès aux données suivant un schéma documenté et exploitable (API, format pivot, etc.).

CLD- 74 Localisation des données personnelles

- Le prestataire doit documenter et communiquer à Pôle Emploi la localisation du stockage et du traitement des données.
- Le stockage, le traitement, ainsi que les opérations d'administration et de supervision des données personnelles de Pôle emploi sont autorisés uniquement dans les pays de l'Union Européenne et au sein des pays reconnus comme adéquats par la Commission Européenne (cf. liste des pays autorisés sur le site internet de la CNIL).

CLD- 75 Questionnaire sécurité sur l'externalisation des données PE

- Le prestataire s'engage à remettre au RSSI de Pole emploi le questionnaire dument rempli concernant l'externalisation de données, fourni dans le dossier de consultation.
- L'appréciation des mesures de sécurité mises en place sera déterminante dans le choix du titulaire.

CLD- 76 Fin de contrat et/ou de partenariat

- À la fin du contrat liant le prestataire et Pôle Emploi, que le contrat soit arrivé à son terme ou pour toute autre cause, le prestataire doit assurer un effacement sécurisé de l'intégralité des données de Pôle Emploi.
- Cet effacement peut être réalisé suivant l'une des méthodes suivantes :
  - effacement par réécriture complète de tout support ayant hébergé ces données;
  - effacement des clés utilisées pour le chiffrement des espaces de stockage de Pôle Emploi;
  - recyclage sécurisé.

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi

- A la fin du contrat, le prestataire doit supprimer les données techniques relatives à Pôle Emploi (annuaire, certificats, configuration des accès, etc.).

3. ANNEXE

3.1. LISTES DES RÈGLES

CLD- 01 GUIDE D'HYGIÈNE DE L'ANSSI 6
CLD- 02 POLITIQUE DE SÉCURITÉ DE L'INFORMATION 6
CLD- 03 ANALYSE DE RISQUES 6
CLD- 04 FONCTIONS ET RESPONSABILITÉS LIÉES À LA SÉCURITÉ DE L'INFORMATION 7
CLD- 05 RELATION AVEC LES AUTORITÉS 7
CLD- 06 RELATION AVEC LES GROUPES DE TRAVAIL SPÉCIALISÉS 7
CLD- 07 LA SÉCURITÉ DE L'INFORMATION DANS LA GESTION DE PROJET 7
CLD- 08 RUPTURE, TERME OU MODIFICATION DU CONTRAT DE TRAVAIL 8
CLD- 09 SENSIBILISATION ET FORMATION À LA SÉCURITÉ DE L'INFORMATION 8
CLD- 10 PROPRIÉTÉ DES ACTIFS 9
CLD- 11 IDENTIFICATION DES BESOINS DE SÉCURITÉ DE L'INFORMATION 9
CLD- 12 MARQUAGE ET MANIPULATION DE L'INFORMATION 9
CLD- 13 GESTION DES SUPPORTS AMOVIBLES 9
CLD- 14 ENREGISTREMENT ET DÉSINSCRIPTION DES UTILISATEURS 10
CLD- 15 POLITIQUES ET CONTRÔLE D'ACCÈS 10
CLD- 16 GESTION DES DROITS D'ACCÈS 10
CLD- 17 REVUE DES DROITS D'ACCÈS UTILISATEURS 10
CLD- 18 GESTION DES AUTHENTIFICATIONS DES UTILISATEURS 11
CLD- 19 ACCÈS AUX INTERFACES D'ADMINISTRATION 11
CLD- 20 RESTRICTION DES ACCÈS À L'INFORMATION 12
CLD- 21 CHIFFREMENT DES DONNÉES STOCKÉES 13
CLD- 22 PROCÉDURE D'ALERTE 13
CLD- 23 PROCÉDURES D'EXPLOITATION DOCUMENTÉES 14
CLD- 24 GESTION DES CHANGEMENTS 14
CLD- 25 SEPARATION DES ENVIRONNEMENTS DE DEVELOPPEMENT, DE TEST ET D'EXPLOITATION 14
CLD- 26 SAUVEGARDE DES INFORMATIONS 14
CLD- 27 MESURES CONTRE LES CODES MALVEILLANTS 15
CLD- 28 JOURNALISATION DES ÉVÉNEMENTS 15
CLD- 29 PROTECTION DE L'INFORMATION JOURNALISÉE 15
CLD- 30 SYNCHRONISATION DES HORLOGES 15
CLD- 31 ANALYSE ET CORRÉLATION DES ÉVÉNEMENTS 16
CLD- 32 INSTALLATION DE LOGICIELS SUR DES SYSTÈMES EN EXPLOITATION 16
CLD- 33 GESTION DES VULNÉRABILITÉS TECHNIQUES 16
CLD- 34 ADMINISTRATION 16
CLD- 35 CARTOGRAPHIE DU SYSTÈME D'INFORMATION. 17
CLD- 36 CLOISONNEMENT DES RÉSEAUX 17
CLD- 37 SURVEILLANCE DES RÉSEAUX 17

CLD- 38 CHIFFREMENT DES FLUX 18
CLD- 39 NON RÉPUDIATION 18
CLD- 40 GESTION DES SECRETS 18
CLD- 41 PÉRIMÈTRES DE SÉCURITÉ PHYSIQUE 19
CLD- 42 CONTRÔLE D'ACCÈS PHYSIQUE 19
CLD- 43 PROTECTION CONTRE LES MENACES EXTÉRIEURES ET ENVIRONNEMENTALES 19
CLD- 44 SÉCURITÉ DU CÂBLAGE 20
CLD- 45 MAINTENANCE DES MATÉRIELS 20
CLD- 46 SORTIE DES ACTIFS PÔLE EMPLOI 20
CLD- 47 RECYCLAGE SÉCURISÉ DU MATÉRIEL 20
CLD- 48 POLITIQUE DE DÉVELOPPEMENT SÉCURISÉ 21
CLD- 49 PROCÉDURES DE CONTRÔLE DES CHANGEMENTS DE SYSTÈME 21
CLD- 50 REVUE TECHNIQUE DES APPLICATIONS APRÈS CHANGEMENT EN PRODUCTION 21
CLD- 51 ENVIRONNEMENT DE DÉVELOPPEMENT SÉCURISÉ 21
CLD- 52 DÉVELOPPEMENT EXTERNALISÉ 21
CLD- 53 TEST DE LA SÉCURITÉ ET CONFORMITÉ DU SYSTÈME 22
CLD- 54 PROTECTION DES DONNÉES DE TEST 22
CLD- 55 IDENTIFICATION DES TIERS 23
CLD- 56 LA SÉCURITÉ DANS LES ACCORDS CONCLUS AVEC LES TIERS 23
CLD- 57 SURVEILLANCE ET REVUE DES SERVICES DES TIERS 23
CLD- 58 GESTION DES CHANGEMENTS APPORTÉS DANS LES SERVICES DES TIERS 23
CLD- 59 ENGAGEMENTS DE CONFIDENTIALITÉ 23
CLD- 60 RESPONSABILITÉS ET PROCÉDURES 24
CLD- 61 SIGNALEMENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION 24
CLD- 62 APPRÉCIATION DES ÉVÉNEMENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ET PRISE DE DÉCISION .. 24
CLD- 63 RÉPONSE AUX INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION 24
CLD- 64 TIRER DES ENSEIGNEMENTS DES INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION 24
CLD- 65 RECUEIL DE PREUVES 25
CLD- 66 ORGANISATION DE LA CONTINUITÉ D'ACTIVITÉ 25
CLD- 67 MISE EN ŒUVRE DE LA CONTINUITÉ D'ACTIVITÉ 25
CLD- 68 VÉRIFIER, REVOIR ET ÉVALUER LA CONTINUITÉ D'ACTIVITÉ 25
CLD- 69 DISPONIBILITÉ DES MOYENS DE TRAITEMENT DE L'INFORMATION 25
CLD- 70 IDENTIFICATION DE LA LÉGISLATION ET DES EXIGENCES CONTRACTUELLES APPLICABLES 26
CLD- 71 REVUE INDÉPENDANTE DE LA SÉCURITÉ DE L'INFORMATION 26
CLD- 72 CONFORMITÉ AVEC LES POLITIQUES ET LES NORMES DE SÉCURITÉ 26
CLD- 73 RÉVERSIBILITÉ 27
CLD- 74 LOCALISATION DES DONNÉES PERSONNELLES 27
CLD- 75 QUESTIONNAIRE SÉCURITÉ SUR L'EXTERNALISATION DES DONNÉES PE 27
CLD- 76 FIN DE CONTRAT ET/OU DE PARTENARIAT 27

Confidentialité : Diffusion interne – Reproduction interdite sans accord préalable de Pôle emploi