Plan d’assurance Sécurité

ANNEXE IBM

cegid

SOMMAIRE

Table des matières

1. ÉVOLUTIONS DU DOCUMENT

Version	Date de publication
PAS_CEGID_SAAS_ANNEXE_IBM_V2017-11	03 novembre 2017
PAS_CEGID_SAAS_ANNEXE_IBM_V2019-05	23 Mai 2019
PAS_CEGID_SAAS_ANNEXE_IBM_V2020-10	7 octobre 2020

2. INTRODUCTION

2.1 Objet

Ce document annexe au PAS décrit les engagements pris par Cegid en termes de sécurité de l'information sur les services opérés sur la plateforme IBM.

2.2 Domaine d'application

Cette annexe s'applique uniquement aux éléments cloud de la plateforme IBM intégrés par Cegid pour délivrer de manière optimisée et opérés par Cegid Cloud Factory.

IBM est considéré par Cegid Cloud Factory comme un fournisseur critique.

2.3 Définitions

ISO : International Organisation for Standardization - Organisation Internationale de Normalisation qui a pour but de produire des normes internationales dans les domaines industriels et commerciaux.

2.4 Documents de références

P.A.S : Plan Assurance Sécurité – Document de base décrivant la politique de sécurité mise en place par Cegid sur la délivrance des services applicatifs à destination de ses clients

Livrets Service : Documents décrivant les conditions particulières liées à chaque offre SaaS de Cegid. Ils sont disponibles sur www.cegid.com, site web de Cegid.

3. Roles et responsabilites

Dans le cadre de son partenariat avec Cegid, IBM met à disposition des ressources dédiées (infrastructures, maintenance, support…) permettant la délivrance du service. Les clauses de sécurité sont consignées dans un document contractuel (CSD) révisé annuellement.

Les engagements de Cegid sur les SLA clients sont indépendants des clauses contractuelles entre Cegid et IBM.

4. Certifications de la Plateforme IBM

Afin de proposer un niveau de sécurité optimal, les Datacenters IBM utilisés par Cegid sont tous Tiers III+.

Les Datacenters en région parisienne ainsi que celui situé à Montpellier sont certifiés ISO27001 et ISO 9001.

5. Gestion des actifs

4.1 Gestion des supports et matériels affectant des données clients

4.1.1 Mise au rebut

Dans le cadre du Cloud Privé de Cegid, les médias (disques durs, bandes magnétiques) contenant des données sont obligatoirement détruits de manière physique (broyage ou poinçonnage) lors d'une mise au rebut ou d'une panne. Un compte rendu est fourni lors des comités sécurité de suivi avec le fournisseur.

Les documents papiers contenant des informations confidentielles sont broyés avant d'être jetés.

6. Securites physiques et environnementales

5.1 Localisation

Les Datacenters utilisés par Cegid sont situés en France. Ils sont répartis en région parisienne, en région lyonnaise et à Montpellier.

5.2 Datacenters

5.2.1 Sécurité physique des sites

Une présentation des Datacenter du Cloud Privé Cegid/IBM est accessible via :

https://www.youtube.com/watch?v=dELnaDsCcjQ

5.2.2 Contrôle d'accès

Chaque accès fait l'objet d'une traçabilité et est validé par un processus dédié. Les journaux d'accès aux salles sont revus trimestriellement avec le fournisseur lors du Comité de pilotage de la sécurité.

7. SECURITE LIEE A L'EXPLOITATION

6.1 Données

6.1.1 Chiffrement des données

Les données sont conservées sur des équipements dédiés par IBM à Cegid.

Cegid applique un chiffrement matériel : les baies de stockage sont chiffrées avec l'algorithme AES 256. Les clés sont gérées par Cegid au travers un Key Management System dédié pour Cegid.

6.2 Sauvegarde

6.2.1 Principe d'externalisation

L'externalisation des données a pour but la protection de l'intégrité physique des supports de données.

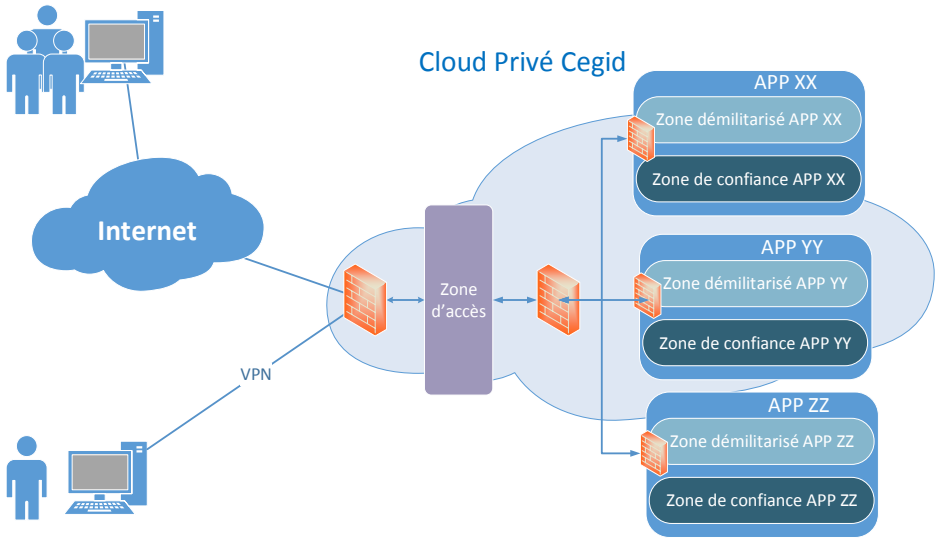
Le Datacenter qui contient les données de sauvegarde est distant de plus de 20km du site principal.

Le transfert des données entre les deux Datacenters se fait uniquement au moyen d'une liaison fibre optique dédiée et privée. Il n'y a donc pas de transport physique de médias contenant des données.

8. SECURITE DES COMMUNICATIONS

7.1 Architecture technique

Les flux entre chaque zone sont contrôlés par des pare-feu.



Légende

Bulles APP XX, YY, ZZ : Bulles applicatives qui correspondent à un ensemble de zones regroupées pour faire fonctionner une application de manière autonome et sécurisée. Cette architecture permet d'assurer l'isolation entre les différents services SaaS.

Zone de confiance (TRZ) : Zone sécurisée contenant les applications et les données de production.

Zone démilitarisée (DMZ) : Zone intermédiaire contenant les services frontaux des applications. Cette zone permet de créer un sas entre les zones d'accès (internet et VPN) et les zones de confiance.

7.2 Accès télécom

7.2.1 VPN

Afin de prévenir le risque d'indisponibilité, les points d'accès VPN de Cegid sont doublés et le matériel utilisé est redondé.

9. GESTION DE LA CONTINUITE D'ACTIVITE

8.1 PCA & Résilience

8.1.1 DRaaS

Le Service DraaS est une option contractuelle permettant au client sur certaines offres de bénéficier d'une reprise d'activité de tout ou partie de leur service SaaS sur un site de secours, en cas de sinistre majeur (destruction) sur le site de production entrainant une indisponibilité prolongée du service de plus de 24 heures et ne permettant pas à Cegid de déterminer avec certitude un délai de reprise d'activité sur le site de production. Le Service DraaS Cegid s'appuie sur une solution technique de réplication continue des données client sur le site de secours.

Les conditions d'exécution (RTO, RPO, périmètre, processus etc…) sont décrites dans les Livrets Service correspondants.

8.2 RPO & RTO

8.2.1 RPO

RPO : Recovery Point Objective ou Point de Rétablissement des données

Lorsque le service DraaS est activé un RPO différent peut régir le Service. Le RPO est défini dans ce cas dans les Livrets de Service correspondants.

8.2.2 RTO

RTO : Recovery Time Objective ou Temps de Rétablissement du service

Lorsque le service DraaS est activé, Cegid s'engage sur un RTO fixé dans les Livrets Service correspondants.