Information Security Practises

IBM APPENDIX

cegid

CONTENTS

1. Document versions

Version	Issue date
PAS_CEGID_SAAS_ANNEXE_IBM_V2017-11	03 november 2017
PAS_CEGID_SAAS_ANNEXE_IBM_V2019-09	09 September 2019

2. Introduction

2.1 Purpose

This appendix to the ISP describes the data security commitments made by Cegid on the services operated on the IBM platform.

2.2 Scope

This appendix only applies to the cloud elements of the IBM platform which Cegid has integrated to deliver the application services selected by the Client in a secure and optimal way.

Cegid's Cloud Factory considers IBM as a critical supplier.

2.3 Définitions

ISO : International Organization for Standardization, whose purpose is to produce international standards in industrial and commercial fields.

2.4 Reference documents

I.S.P : Information Security Practises - Basic document describing the security policy implemented by Cegid for providing application services to its clients.

Terms of Service : Document describing the specific conditions related to each of Cegid's SaaS services. These are available on www.cegid.com, Cegid's website.

3. IBM plateform Certifications

In order to offer an optimal service, the IBM datacenters used by Cegid are all Tiers III+.

Datacenters in the Paris region as well as those in Montpellier are ISO27001 and ISO 9001 certified.

4. Asset management

4.1 Managing media and equipment that have an impact on client data

4.1.1 Scrapping

In Cegid's Private Cloud, media (hard disks, magnetic tapes) containing data must be destroyed physically (shredding or punching) if subject to scrapping or failure. A report is providing during monitoring security committee meetings with the supplier.

Hard copies containing confidential information are shredded before being disposed of.

5. Environmental and physical security

5.1 Localisation

The datacenters used by Cegid are located in France. They are in the regions of Paris, Lyon and in Montpellier.

5.2 Datacenters

5.2.1 Physical security of sites

presentation of the Cegid/IBM private Cloud Data centre is accessible via :

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

5.2.2 Access management

This access is subject to traceability and is validated by a dedicated process. The access logs for the rooms are reviewed quarterly with the supplier during the Security steering committee meeting.

6. Operational security

6.1 Data

6.1.1 Data encryption

Data is held on the SaaS platform in secure zones, both for storage and backup. In this context, encryption is not therefore implemented..

6.2 Backup

6.2.1 Outsourcing principle

Data outsourcing aims to protect the physical integrity of data media.

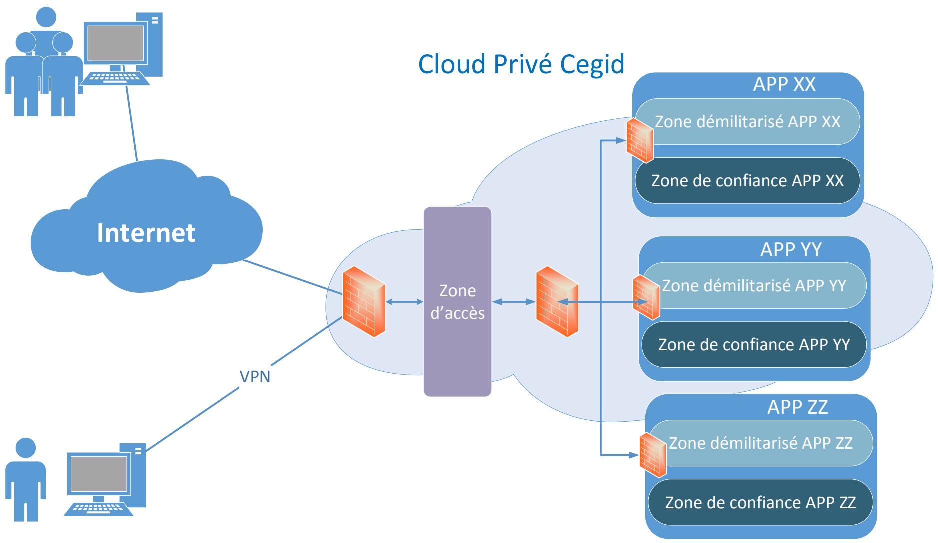
The data center which holds the backup data is more than 20km from the main site.

Data is transferred between the two Data centres only through a private, dedicated optical fibre-link. There is therefore no physical transport of the media containing the data.

7. Communication security

7.1 Technical architecture

Flows between each zone are controlled by firewalls.



Legend

APP XX, YY, ZZ bubbles: Application bubbles which correspond to a set of grouped zones to run an application automatically and in total security. This architecture makes it possible to ring fence the different SaaS services.

Trust zones (TRZ) : Secure zones containing production applications and data.

Demilitarized Zone (DMZ) : Intermediary zone containing front-end application services. This zone creates an airlock between the access zones (internet and VPN) and the trust zones.

7.2 Telecom access

7.2.1 VPN

In order to prevent the risk of unavailability, Cegid's VPN access points are doubled, and the hardware is redundant.

8. Management of business continuity

8.1 BCP & Resilience of SaaS services

8.1.1 DRaaS

The DRaaS service is a contractual option giving the clients of certain services the ability to recover all or part of their SaaS service from a recovery site, if there is a major disaster (destruction) on the production site resulting in the prolonged service unavailability of more than 24 hours for which Cegid is unable to be certain of a time to recovery. Cegid's DRaaS uses a technical solution of Continuous Replication of client data on the recovery site.

The operating conditions (RTO, RPO, scope, procedures, etc.) are described in the related Terms of Service.

8.2 RPO & RTO

8.2.1 RPO

RPO : Recovery Point Objective

When the DRaaS service is activated a different RPO may govern the Service. In this case, the RPO is set out in the related Terms of Service.

8.2.2 RTO

RTO : Recovery Time Objective

When the service DraaS is activated, Cegid commits to a RTO that is set in the related Terms of Service.