Information Security Practises

Cegid SaaS

cegid

CONTENTS

1. DOCUMENT VERSIONS

Version	Issue date
PAS_CEGID_SAAS_V2017-11_CLIENT_V.EN	03 November 2016
PAS_CEGID_SAAS_V2018-02_CLIENT_V.EN	02 February 2018
PAS_CEGID_SAAS_V2018-07_CLIENT_V.EN	30 July 2018
PAS_CEGID_SAAS_V2019-08_CLIENT_V.EN	28 August 2019

2. INTRODUCTION

2.1 Purpose

The Information Security Practices (ISP or PAS (French term)) describes the information security commitments taken by Cegid (availability, integrity, confidentiality and traceability) for the SaaS services that it provides.

2.2 Scope

This document applies to the :

- SaaS services provided by Cegid Cloud Factory
- Management tasks performed by Cegid Cloud Factory
- Cegid SaaS Production services provided in partner-supplier Data Centers

2.3 Definitions

Assets : All the goods or services which make it possible for Cegid to provide SaaS services

BSI : British Standard Institution

CERT : Computer Emergency Response Team

CMP : Cloud Management Platform

CNIL : Commission Nationale Informatique et Liberté

DCP & DRP: Disaster Continuity Plan & Disaster Recovery Plan

IPS : Intrusion Prevention System

ITSM : Information Technologie Service Management

Terms of Service: Document describing the specific conditions related to each of the Cegid SaaS services.

Cloud Factory : Organisation within Cegid responsible for designing, operating and providing technical support for Cegid's SaaS platform (cf. Presentation of Cloud Factory)

ISO : International Standard Organization

OWASP : Open Web Application Security Project

ISSP : : Information Systems Security Policy

GDPR : General Data Protection Regulation

RPO : Recovery Point Objective

CISO : Chief Information Security Officer

RTO : Recovery Time Objective

ISMS : Information Security Management System. This term refers to a set of policies related to the management of information security

VM : Virtual Machine

VPN : Virtual Private Network

2.4 Reference documents

ToU : Terms of Use -This document is available on www.cegid.com, Cegid's website

ISO 27001 : Standard setting requirements for Information Security Management

ISO 27002 : Best practice recommendations for ISMS

ISO 27005: Standard for risk management for information security

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. Presentation of Cloud Factory

The Cloud Factory is a department within the Cegid Group responsible for making applications in SaaS (Software as a Service) mode available for the Cegid group's clients.

The main roles of this team are :

- Designing the architecture necessary for hosting applications and data
- Operating hardware, software and network architecture
- Operating the applications
- Providing technical support for the SaaS services.

4. Best practices and ISO 27001 certification

Cegid's security requirements with regards to its services provided to clients are expressed by implementing an ISM system.

The purpose is to protect the features and data from any loss, theft or alteration and protect information systems from any intrusion or disaster.

By applying best practices and implementing the continuous improvement process, Cegid's ISM has been awarded the ISO 27001 certification (Certificate no. IS 666376 issued by BSI) on the following scope:

> Application hosting services in a Cloud environment, containing data provided by the clients.

This scope certifies the service provision process, from orders to release. It does not extend to application development.

The sections in this document cover the security requirements for this standard.

5. Risk management

Cegid's Cloud Factory teams have implemented a risk management process based on the ISO 27005 standard's principles. It has three phases:

- Risk analysis

- Action and risk resolution plan created in cooperation with all the teams
- Regular monitoring and supervision (reviewing action plans during operational and strategic committee meetings under the responsibility of the Data Security Manager and his team).

As part of the continuous improvement policy, risk analysis is repeated each year.

6. INFORMATION SECURITY POLICY

Cegid's SaaS business is governed by an information Systems Security Policy (ISSP). This policy was implemented in 2008 and is revised annually. It is based on the principles of best practices of the ISO 27001 and ISO 27002 standards.

This policy aims to protect the critical data of Cegid's Cloud Factory, its clients and its partners.

The security policy is published in the internal document control tool and everyone concerned is automatically informed of any revisions.

This policy is confidential and cannot be circulated. This document (Security Plan) reproduces the plan and the data that can be disseminated.

In order to maintain the security and integrity of its platforms, Cegid does not disclose the names or information related to the security aspects implemented (suppliers, publishers, etc.).

The Information Security Practises is revised at least annually.

7. ORGANISING INFORMATION SECURITY

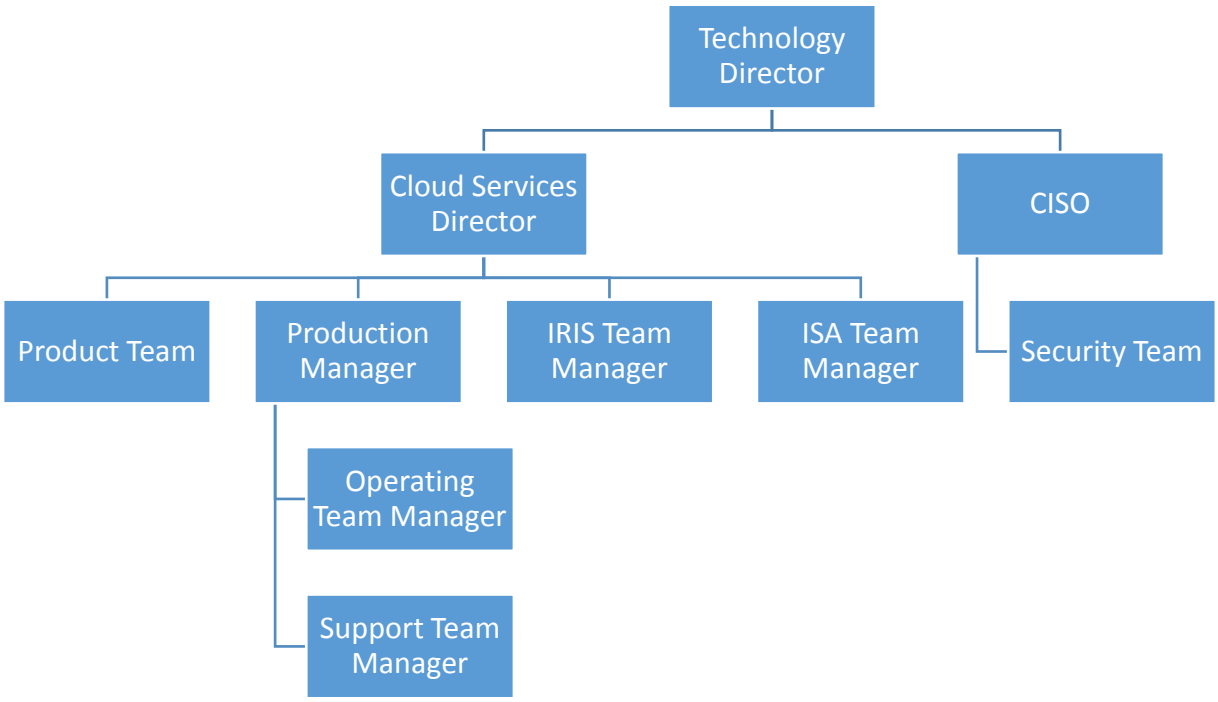
7.1 Internal organisation

7.1.1 Roles et responsabilities

Responsibilities for security have been set and assigned.

An CISO is appointed with responsibilities for all the Cegid group's business. A security team reports directly to the ISSM.

Staff involved in data security are:



7.1.2 Separation of tasks and areas of responsibility

In order to reduce the risk of (unauthorised or accidental) modification or damage to the assets the tasks and areas of responsibility for teams are broken down by function.

SECURITY TEAM : Operational security and continuous improvement of the ISMS

PRODUCT TEAM: Interface with the group's sales and marketing entities, integrating and upgrading services, management and CMP, etc.

OPERATING TEAM: Managing the life cycle of the services provided (introduction, monitoring, decline).

SUPPORT TEAM: Incident handling.

IRIS TEAM: Designing, administrating and documenting system and network architectures as well as the necessary tools for the services.

ISA TEAM: Designing, administrating and documenting application architectures and production tools (automation, industrialisation).

7.1.3 Governance

Governance bodies have been set up at the strategic (Strategic Information Security Committee) and operational (Operational Information Security Committee) levels.

These bodies meet regularly to monitor information systems security issues. Meeting reports are stored in the document control system.

7.1.4 Relations with organisations and authorities

Cegid is a member of CLUSIR (Clubs de la sécurité de l'information régionaux) Rhône-Alpes, de l'OzSSI (observatoires zonaux de la sécurité des systèmes d'information) and maintains relations with the authorities in order to monitor changes in the information security field.

7.1.5 Security intelligence

Security intelligence is part of Cegid's SaaS business. Its aim is to prevent risks specifically related to the SaaS business.

Cegid also draws on the services of companies specialised in security intelligence (CERT) to increase its research capabilities. By having multiple research methods, it is possible to cross-reference information found and receive tailored, pertinent results in the specific SaaS context.

8. HUMAN RESOURCES SECURITY ISSUES

8.1 Recruitment

Employment candidates' information is checked in accordance with regulations, ethical standards, laws, and any appropriate legislation in force in the jurisdiction concerned. They are proportional to employment requirements, classifying accessible data and identified risks.

Checks include the following points:

- Professional references
- Checking the exhaustive nature and exactitude of the candidate's curriculum vitae
- Copies of the degree, training and professional qualification certificates, mentioned in the CV,
- Independent identity check, passport or identity card.
- Checking the criminal record
- Checking that the work permit, residence card is valid, if the candidate is an immigrant

These checks are also applicable to contractors and temporary staff.

8.2 Managing confidentiality

All the staff in SaaS Production are made aware of security issues.

Each contract stipulates and specifies the following points:

- Intellectual Property Compliance
- Compliance with the legislation on protecting personal data
- Protecting data, data assets, company applications
- Protecting data from partners and other organisations or third-parties

Our internal rules and regulations, given to and signed by each employee during the recruitment process, also stipulates the confidentiality rules as well as the proper way to use the tools provided (Email/messaging system, Internet).

Specific provisions may apply in the following situations:

- The initiation of a formal disciplinary process (known to all employees) against employees who have breached the information security rules. This is a dissuasive factor which prevents employees and contractors from breaching the company's security policies and procedures as well as any other security rule. Deliberate breaches of these rules will trigger its immediate activation
- Non-observance of the different clauses following which, a formal, known disciplinary process will be activated.
- The responsibilities stated in the employment contract will continue to apply during a set period after the contract ends.

There is a plan for building confidentiality awareness and business confidentiality compliance which is managed by the CISO and the security team.

8.3 Skills management

8.3.1 Security awareness

New employees in SaaS Production follow an integration programme presented by the Chief Information Security Officer or someone from the security team which includes security and confidentiality awareness plan.

Regular awareness training sessions, aimed at all staff in SaaS Production, are then carried out via presentation sessions or information emails.

8.3.2 Skills and training

To maintain know-how, identify training needs and organise knowledge sharing, Cegid has set up a skills management programme for all the staff in Cloud Factory.

9. ASSET MANAGEMENT

9.1 Inventory

Cegid's Cloud Factory sets up an inventory of the essential assets and support assets. These are listed in the risk analyses in order to be able to centralise all the associated risks.

A set of characteristics and properties are stored such as the identifying codes, configurations, etc.

An automated updating process reconciles the inventory and the assets in the SaaS scope.

9.2 Identifying assets

Each asset is assigned to an owner.

The assets used for providing SaaS services are based on a formal naming convention, without any distinctive sign that would make it possible to create a direct link with the clients.

9.3 Document control

All Cegid's Cloud Factory process and functional documents are listed and classified in an EDM. Access to these documents is restricted to staff in Cloud Factory, and internal or external auditors.

9.4 Managing media and hardware that have an impact on client data

9.4.1 Storage

Removable media containing client data is stored in a secure location when not in use.

9.4.2 Physical transfer

For any physical transfer of media containing confidential data, SaaS Production exclusively uses well known and reliable courier companies that provide tracking and proof of delivery. When SaaS Production has to return data on storage media sent by the client, it will be sent using the same techniques and methods used when initially sent.

9.4.3 Scrapping

Asset scrapping is subject to a specific procedure to remove confidential data. This procedure requires the secure removal or physical destruction of media which contains confidential data.

9.4.4 Maintenance

Liability for hardware extends to Cegid's cloud infrastructure suppliers..

9.5 Managing Cloud Factory staff's hardware

9.5.1 Equipment maintenance

The staff workstations in SaaS Production are supplied by Cegid group. They are maintained and updated by the supplier through a leasing service on these machines.

9.5.2 Scrapping

Any storage media present in the scrapped hardware is destroyed securely according to applicable procedures (data erasure software that uses the Guttman method / DoD 5220.22M)

9.5.3. Managing removable media

The security policy for removable media implemented and managed by a software such as Endpoint, can only be used by a single type of removable media (identified and validated USB flash drive).

10. OPERATING SYSTEM SECURITY POLICY

A hardening policy to secure operating systems is implemented. The aim is to reduce the possible attack surface, by disabling or removing non-essential objects (services, applications,

functionalities, etc.). This consists of setting up specific security options and ensuring software updates.

10.1 Microsoft operating system

- Update
- Account strategy
- User and network rights
- Audits and logs
- Antivirus and anti-malware
- Service role and functionality

10.2 Linux operating system

- User space
- Disk space
- Update
- Logs

11. ACCESS MANAGEMENT

11.1 Password management

Each user is authenticated by a unique ID and strong password.

Users passwords are encrypted when stored on Cegid's SaaS platform and they use non reversible encryption features such as 'hashing' by the Windows Active Directory.

11.1.1 Policy for Cloud Factory administrators

Passwords for Cegid's Cloud Factory administrators are subject to a strict security policy:

- Minimum size: 10 characters
- Complexity: letter, figure and symbol
- Frequency of change: every 60 days
- No reuse of the last 24 passwords
- Lockout after 5 attempts (unlocked by a Cloud Factory administrator)

11.1.2 Policy for Cegid's SaaS clients

The standard policy for user passwords of Cegid's SaaS clients is as follows:

- Minimum size: 8 characters
- Complexity: letter, figure and symbol
- Frequency of change: every 90 days
- No reuse of the last 24 passwords
- Lockout after 5 attempts (unlocked by a Cloud Factory administrator or a user via an online password management tool)

11.2 Managing rights

Rights management for the SaaS Production teams are based on the "least privilege" principle. Each team only has the rights necessary for the tasks that they perform.

Requesting rights (adding, modifying, removing) is done via work flows tracked and approved by the security team.

The list of SaaS Production teams who can access the infrastructure and the SaaS solutions are:

- Operating team: 8 Employees
- IRIS team (infrastructure et network) : 13 Employees
- ISA team (database and application) : 13 Employees
- Support team: 10 Employees
- Product team : 4 Employees
- Security team: 4 Employees

In the interests of confidentiality, no personal data relating to Cegid's Cloud Factory staff will be disseminated.

11.3 Removing access

Removing access rights for Cegid staff is related to the HR process when staff leave. This is monitored and tracked via an internal workflow.

11.4 Reviewing rights

Rights are reapproved for SaaS Production administrators on a quarterly basis by the SaaS security team. This makes it possible to check and guarantee that the security rules are correctly applied.

12. CRYPTOGRAPHY

12.1 Data transfers

During transfers, data is encrypted with secure protocols. The SaaS platform uses the following protocols:

- HTTPS (TLS)
- SFTP (SSH)

In case of removable media (USB keys or disks), the data are encrypted by the customer with the help of Cegid support team before shipping. If it is not the case, then, the customer is responsible for the security of his data during the shipment to Cegid. After the data integration, the content of the media is erased before being returned to the customer.

If confidential data transfer must transit via non-secure links or media (e.g. email, removable media), these must be encrypted by complying with the rules in force (see § Encryption).

12.2 Certificates

In order to guarantee the highest level of security, HTTPS certificates used by Cegid come from public, recognised authorities. The certificates implemented use 2048-bit keys and a SHA-256 signature in accordance with current best practices.

The procedures for managing certificates shall cover the following aspects:

- Secure issuance of certificates (verification of user identity)
- Secure transmission of certificates
- Deactivation and renewal of certificates
- Secure storage and backup of certificates (key Vault)
- Issuance of certificates by an approved body

12.3 Encryption

The rules on the encryption key length are:

- Asymmetrical encryption: higher than or equal to 2048 bits
- Symmetrical encryption: higher than or equal to 128 bits but 256 bits recommended if accepted by the systems

Cegid's Cloud Factory uses an encryption software based on the AES256 to create secure archives.

12.4 Mobility

Cloud Factory administration teams can connect remotely. This access must be done using a secure connection (VPN or secure access interface). Strong authentication based on an OTP (One Time Password) is necessary to connect remotely.

Cegid's Cloud Factory mobile workstations are equipped with a security suite for integral encryption of hard disks. This encryption uses the (XTS-AES, AES-CBC) protocol.

13. ENVIRONMENTAL AND PHYSICAL SECURITY

13.1 Location

The datacenters used by Cegid are located around the world. Cegid ensures that its suppliers are compliant on both legal and technical issues.

The management center for Cegid's Cloud Factory is based in Lyon.

13.2 Datacenter security

13.2.1 Physical security of sites

In order to offer the highest security levels, the datacenters used by Cegid are all 1SO 27001 certified. The following characteristics are taken into account:

- Electricity
- Air conditioning
- Fire protection
- Alarm, security, CCTV, etc.

13.2.2 Equipment security

A range of measures and principles have been put in place at the design level of the infrastructure in order to provide the optimal level of availability and integrity needed for Cegid's SaaS services.

The main rule is to avoid any SPOF (Single Point of Failure) on the hardware or links.

For example:

- Redundancy at the physical server level
- Redundancy at the network level
- At the storage level

- Virtualisation

13.2.3 Access management

Access to the secure physical facilities which host the system hardware and critical networks is restricted to authorised personnel.

13.3 Cegid Cloud Factory

13.3.1 Site security

Cegid's Cloud Factory offices are subject to the same regulations as the rest of the buildings on the Cegid Lyon Vaise site, which are mainly:

- EDF energy supply with a specific contract & UPS
- Fire detection sensors, extinguishers
- Supply of air conditioning, heating and ventilation serices

13.3.2 Access management

Access to Cegid's Vaise site is via security badges. Each staff member has a programmed badge that gives total or partial access to certain parts of the building.

The badges and access are programmed, managed and centralised by a software administered by the Cegid Vaise's Facilities department

Access to Cegid's Cloud Factory buildings is managed in a software by a specific group and provided on demand or validated by the security team.

Cegid Vaise premises are fitted with an alarm system

Visitors to the site are subject to a specific procedure managed jointly by the Cegid's facilities department and the security team in order to check their identity.

13.3.3 Clean desk

A clean desk policy is in place in the offices of Cloud Factory teams. Documents, media or any other support which may contain confidential information are stored when they are not in use.

14. OPERATIONAL SECURITY

14.1 Data

14.1.1 Data classification

The ISO 27001 standard requires a classification of essential goods and information. This classification is based on three criteria:

- Public
- Limited
- Confidential

In this context, customer data is classified as "Confidential".

14.1.2 Data ownership

Data ownership is not delegated when using Cegid's SaaS services. The client remains the only owner of its data, as specified in the Terms of Service.

14.1.3 File security

Data files are stored in specific directories for each of our clients. These directories are protected with NTFS security systems or similar.

Cegid can therefore guarantee the security, partitioning and impermeability for each client.

14.1.4 Database security

Cegid uses standard or well-known systems such as Microsoft SQL, Oracle or MySQL for its databases.

By selecting major providers, Cegid can have access to experienced software publishing houses, and a very active community in order to always maintain its database management systems at the optimal level.

14.1.5 Data encryption

Data is secure when transferred between the user workstation and Cegid's SaaS platform, by using encryption protocols such as HTTPS or SFTP.

14.1.6 Data integrity

Cegid undertakes to provide protection against data damage or destruction (deliberate or accidental), through secure procedures and protocols for sending and storing its clients' data.

14.1.7 Agreement termination

The methods for retaining or deleting client data after an agreement is terminated are provided in the Terms of Service for the SaaS services.

14.1.8 Managing changes

Changes made to the business processes, systems, and methods for handling data are centralised. They are subject to a weekly review during Production meetings.

14.2 Antivirus

All the server infrastructure is protected by a central antivirus and antimalware software. The pivot server checks at least once a day that the publisher has performed an update. Updates are then disseminated to all servers.

Antivirus monitoring is included in Cegid's SaaS platform monitoring and is one of the principal indicators reviewed during information security meetings.

14.3 Backup

14.3.1 Backup policy

Cegid's SaaS Production teams are primarily focussed on our clients' data. In order to ensure the integrity and availability of client data, Cegid uses a powerful backup system.

Cegid operates on the principle of a double backup.

The first backup is done from the production systems on an initial dedicated infrastructure.

A duplicate is then made on a second dedicated infrastructure.

Backup facilities are not located in the same datacenter as the production systems. In this way, it is possible to guarantee optimal availability and integrity while meeting our RPO requirements (see §RPO).

The backup frequency is specific to each service and detailed in the Terms of Service of the relevant service.

14.3.2 Checks and recovery

The monitoring software runs checks on the backup tasks. If there is an incident during a backup, an automatic alert is sent, and this is handled by Cegid's Cloud Factory teams.

As part of its regular operating activity, Cloud Factory performs recoveries on a daily basis. These make it possible to validate that the backups as well as the associated recovery procedures are working correctly.

14.3.3 Retention principle

As a specialised software publisher, Cegid has an in-depth understanding of its clients' needs. This characteristic has enabled us to implement a specific backup retention period for each of our proposed services.

These retention principles are detailed in the Terms of Service for each service.

14.4 Trace management

14.4.1 Collecting traces

Traceability on Cegid's SaaS platform is provided by a concentration and correlation tool for logs. This is kept for 1 year for technical and operational purposes.

This tool makes it possible to standardise the retention period for data collected and to guarantee its security.

The data collected include user name, log in/out time, application used, source IP address, etc.

14.4.2 Architecture

The technical architecture supporting this tool provides redundancy and continuous availability of data.

14.4.3 Policy for accessing tools

The tool is accessible as read only for all Cegid Cloud Factory staff.

Access to make changes is restricted to server administrators operating the tool (2 people) and security team members (4 people).

14.4.4 Using traces

Uses of collected data are for:

- Meeting regulatory constraints related to Cegid's business.
- Monitoring the health of Cegid's SaaS platform and rapidly detecting any event that may lead to a drop-in service level.
- Producing statistical data (rendered anonymous) concerning service provision

The use of trace statistics and data is governed by the Terms of Use.

14.5 Monitoring

14.5.1 Principles

All Cegid's services and the SaaS platform are monitored by centralised tools. These tools either use the SNMP protocol or automation developed specifically in order to recover data from all the control points.

Cegid Cloud Factory teams may therefore continuously monitor the health of services and receive real time alerts in the event of a malfunction.

The tools are coupled to a system that sends text messages to teams on-call, out of working hours.

14.5.2 On-call support

The on-call support service is responsible for working on the SaaS platform 24/7. The team includes specialists from every area of expertise within Cloud Factory.

14.6 Managing updates

14.6.1 Managing installed software

Cegid uses a software to make an inventory of and to manage all the software on the SaaS platform as well as on administration work stations.

14.6.2 System update

System updates are performed through a centralised console.

The principle used by Cegid to carry out critical and security updates is as follows: the updates are deployed across all control environments over the 7 days after a patch is released. During this time, the team check if the patch presents a problem to the integrity and/or availability of the service provided to clients. If no problem is identified, the patch is deployed across the whole platform over the following 7 days.

14.6.3 Application update

Cegid executes technical and organisational industrial processes to manage the application updates based on the commitments laid out in the Service Manual of its SaaS solutions.

15. COMMUNICATION SECURITY

15.1 Technical architecture

The infrastructure supporting Cegid's SaaS services is organised into security zones and application zones. This principle makes it possible to offer in-depth security tailored to current and future needs.

15.2 Telecom access

There are 2 access modes for Cegid's SaaS services:

- Virtual Private Network
- Secure Internet

15.2.1 Virtual Private Network

Cegid offers its clients the possibility to make use of a direct, enhanced and secure access to its SaaS services through a private network solution. The availability and characteristics are specified in the technical prerequisites of each SaaS solution.

15.2.2 Internet

Cegid has its own public IP addresses as well as several internet accesses with different suppliers to mitigate any failure of one supplier and therefore provide its clients with the expected service level.

All communication options provided by Cegid are secure. The flows transit in HTTPS and SFTP.

15.3 Security equipment

15.3.1 Firewalls

Firewalls have been set up between each security zone and each application zone.

External flows cross several layers of firewalls before reaching the requested service.

Direct flows to trusted zones are not authorised, they must pass through the demilitarised zones (DMZ).

15.3.2 IPS

IPS sensors are located at the edge of the network to analyse all the inflows and outflows of Cegid's SaaS platform. Their role is to detect abnormal flows and the malicious traffic and to block them.

The sensors recover updates of attack signatures from the publisher's security experts and are deployed under the responsibility of Cegid's Cloud Factory.

15.3.3 Vulnerability scanner

Scans across the entire Internet scope of the SaaS platform are run on a monthly basis via a vulnerability scanner managed by Cegid's SaaS Production security teams. These scans check the proper configuration of the hardware and software in order to prevent any vulnerability appearing.

Results are reviewed and are subject to specific action plans.

15.3.4 High availability and Fault Tolerance

The availability of SaaS services is provided by several load balancing systems. These are present to mitigate a malfunction, failure of a component or temporary unavailability when updating the systems, which are:

- Load balancing in cluster on the network and telecom equipment
- Capacity planning method with hot extend (VM and Firewall)
- Application load balancing on server farms

16. PURCHASING, DEVELOPING AND MAINTAINING IT SYSTEMS

Cegid treats development security as a major issue.

Cegid has set up a community of lead developers in the security field within each development team. This makes it possible to capitalise on security issues and ensure that best practices are disseminated and implemented (such as OWASP).

A development committee as well as working groups between the different Cegid teams involved in the product life cycles manage the continuous improvement process.

Specific security intelligence is carried out and regular newsletters, updates, improvements are sent to teams.

16.1 Environment partitionining

Cegid's SaaS Production networks and infrastructure are physically and logically separated from other networks in the Cegid group.

The platform also separates the different application environments. These can be accessed by teams with the appropriate security levels.

The development environment is exclusively restricted and accessible to developers and contains no production data, excepting any specific contractual agreement with the client.

The pre-production and production environments are restricted and accessible to Cegid's SaaS Production teams based on user profiles and rights.

17. SUPPLIER RELATIONS

For all suppliers:

Security is taken into account when contracting with Cegid.

A document describing the security requirements, roles & responsibilities and indicators between the parties is provided to the supplier.

For critical suppliers:

Security tasks are monitored, and indicators reviewed quarterly.

Audits or certifications are required to ensure that suppliers manage the security of IT systems robustly.

18. INCIDENT MANAGEMENT RELATED TO DATA SECURITY

18.1 Managing security incidents

Security incidents are handled by a workflow in Cegid's SaaS task management tool. The principle is inspired by the best practices in the ISO 27001 and ISO 27002 standards.

It contains the following steps:

- Alert

- Assessment
- Reaction to the incident (containment, contention and mitigation measures)
- Handling the incident (corrective action plans to treat the root causes)
- Post incident handling (implementing preventive actions)

Notice is sent promptly to clients and/or partners concerned once the extent of the impact has been assessed.

Depending on the type of action plan, Cegid can also contact the entities concerned in the group to arrange for the incident to be handled.

18.2 Crisis management

A specific official crisis management plan has been implemented for Cegid's SaaS business.

Crisis scenarios are managed by a specific organisation, procedures and crisis reaction forms. A crisis management directory is common to all scenarios.

A crisis simulation is organised annually based on a pre-defined scenario. Afterwards, a review is held to take account of any changes to Cegid's SaaS business and associated risks.

19. BUSINESS CONTINUITY MANAGEMENT

19.1 Monitoring continuity

A continuity plan is set out in order to manage and monitor the SaaS services (infrastructure, applications, etc.) for the SaaS Production teams.

19.2 PCA & Resilience

Business continuity is taken into account by default in the design phase of Cloud services delivered by Cegid thanks to the baked-in Project Security.

The Business Continuity Plan (BCP) is defined globally in accordance with Cegid Cloud Information Security Policy that is adapted to each business offering based on the constraints and the technical architectures.

Critical resources (Human Resources, Infrastructure, Information System, Intangible Resources) and their risks are identified for each business offering through the ISP.

The BCP is designed to meet the continual business availability requirements defined in the service availability.

Beyond the resilience by design of the technical and software architectures, the BCP operational and organizational processes are defined and tested as part of the continuous improvement process, in accordance with the industry best practices.

19.3 RPO & RTO

19.3.1 RPO

RPO : Recovery Point Objective

Cegid's standard guarantee is a 24h RPO for all its client data.

19.3.2 RTO

RTO : Recovery Time Objective

Cegid does not define a standard RTO in its Terms of Service. In the event of a serious incident leading to a prolonged interruption of service, Cegid commits to recover the Service as quickly as possible, based on the most suitable backup.

20. CONFORMITY

20.1 Standards & regulation

20.1.1 ISO 27001

The Cloud Factory teams refer to ISO 27001 and ISO 27002 standards to design and operate Cegid's SaaS platform.

In order to offer a state-of-the-art security architecture and infrastructure, Cegid uses Data Centers and associated services which are ISO 27001 certified.

20.1.2 ISO 9001

Cegid's cloud infrastructure suppliers are ISO 9001 certified.

20.1.3 CNIL - (French Privacy Protection Authority)

20.1.3.1 Cegid acting as a subcontractor

The Client is responsible for carrying out the procedures, declarations, authorisation requests provided for by the statutory regulation in force concerning any processing that it performs and

data that it handles using the Service, and more specifically, those provided for by CNIL, for processing personal data. Under Act n° 78 -17 of 06 January 1978, the French data protection act, Cegid acts as a subcontractor, on instructions from the client, which accepts liability for any data processing performed via the Service.

More generally, the client is responsible for compliance with any local legislation when specific administrative filing procedures for personal data is required.

20.1.3.2 Cegid acting as a data controler

As part of its business as a SaaS provider, Cegid shall carry out procedures, declarations, authorisation requests for data processing which it performs when it is the data controler as defined by CNIL and French legislation.

Declarations fall under the client's responsibility when the client meets the requirements to be the data controler and Cegid is acting as subcontractor.

20.1.4 GDPR

Cegid has taken into account the new European regulation on the protection of personal data (RGPD/GDPR). A DPO (Data Protection Officer) assisted by a "key user" are in charge of applying this new regulation. They also take charge of all processes related to these obligations, including the processing of incidents related to personal data.

20.2 Audit

20.2.1 Internal audits

The SaaS business is inspected by an (internal or external) consultant under the joint supervision of the security department or the internal audit department.

This team performs an annual risk analysis, and reviews action plans and indicators in line with the group's audit plan.

The documents for the internal audits are confidential and cannot be disseminated. In the event of a non-compliance which affects security, Cegid undertakes to inform the client(s) concerned in the affected scope (see § Managing security Incidents).

20.2.2 External audits

As part of the ISO 27001 certification: 2013, Cegid is audited annually by the certification body.

Cegid also carries out regular technical audits on its SaaS platform.

20.2.3 Client audits

Organisational audits and pen tests can be performed at the client's request. They are subject to certain conditions and requires a specific contractual clause.