cegid

Security Assurance Plan

CEGID

04/03/2024

www.cegid.com

About this document

The aim of this document is to introduce the Cegid Security Assurance Plan.

Confidentiality level	Public
Last updated	04-Mar-2024

CONTENTS

1. MODIFICATIONS TO THE DOCUMENT

The dates in the following table are the document approval dates.

Date	Author	Type of modification
03-Nov-2016	Cegid Security Team	Initial version
02-Feb-2018	Cegid Security Team	Document review
30-Jul-2018	Cegid Security Team	Document review
23-May-2019	Cegid Security Team	Document review
07-Oct-2020	Cegid Security Team	Document review
08-Aug-2022	Cegid Security Team	Merger of the existing Security Assurance Plans into the Cegid plan
31-Mar-2023	Cegid Security Team	Review of the document, addition of relevant offers concerned and typographical corrections
04-Mar-2024	Cegid Security Team	Review of the document, addition of relevant offers concerned and typographical corrections

2. INTRODUCTION

2.1. Purpose of the document

This document constitutes the Security Assurance Plan (SAP), which may be attached to customer contracts. It describes the commitments made by Cegid to meet the contractual Information System (IS) Security requirements aimed at:

- Protecting the IS resources used to carry out the activities and supply the contracted deliverables;
- Protecting the Customer from any damages they may suffer as a result of the unavailability of these resources, a breach of their integrity or their confidentiality.

This Security Assurance Plan (SAP) lists the security-related measures concerning the physical, organisational, procedural and technical measures implemented.

The measures described in this document may be supplemented by those described in the Service Booklet corresponding to the Cegid offer concerned.

2.2. Scope

This document applies to the SaaS services operated and delivered by the Cegid Cloud teams, and to the activities of these teams.

2.3. SAP modifications

Any modifications to the SAP will result in a new version of this document. Modifications are recorded and dated in the version history at the beginning of the document.

A minor modification[1] will not necessarily result in a new version of the SAP being issued immediately. This modification will be incorporated in the next version of the document.

Any modification to the SAP must form part of the SAP and is equally binding on the parties.

Should the document be modified, the version published on the official Cegid website is the reference. The version attached to the customer contract serves to check that there is no regression.

The SAP is reviewed at least once a year. This review may lead to a new version of this document.

1 Modification with no impact on security requirements

2.4. Definitions

Assets: All goods or services used to deliver Cegid's offers

ASVS : Application Security Verification Standard

BSIMM: Building Security In Maturity Model

CAB: Change Advisory Board

Cegid Cloud: Organisation within Cegid responsible for the design, operation and technical support of the Cegid SaaS platform (see Cegid Cloud presentation)

CISO: Chief Information Security Officer

CMP: Cloud Management Platform

Customer: Customer of a solution covered in this document

DPO: Data Privacy Officer

EDM: Electronic Document Management

GDPR: General Data Protection Regulation

IPS: Intrusion Prevention System

ISMS: Information Security Management System. This expression refers to a set of policies concerning information security management

ISO: International Standard Organization

ISSP: Information Systems Security Policy

ITSM: Information Technology Service Management

OWASP: Open Web Application Security Project

PAM: Privileged Access Management

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SAMM : Software Assurance Maturity Model

SAP: Security Assurance Plan

Terms of Service: Document describing the specific conditions for each Cegid SaaS offer

VM: Virtual Machine

VPN: Virtual Private Network

2.5. Reference documents

GTC: General Terms and Conditions of Use for Cegid services. These are available on the Cegid website, www.cegid.com

ISO 27001:2013: Standard on Information Security Management Systems (ISMS) requirements

ISO 27002:2013: Guide to good practices in ISMS

ISO 27005:2018: Information security risk management standard

Terms of Service: Documents describing the specific conditions related to each Cegid SaaS offer. These are available on the Cegid website, www.cegid.com

3. ROLES AND RESPONSIBILITIES

In order to provide its services, Cegid uses the infrastructure made available by its partners. The deployment and maintenance of this infrastructure are under the responsibility of these partners.

4. DESCRIPTION OF THE SERVICES

The application-specific services provided by Cegid and their description are provided in the terms of service.

5. GOOD PRACTICE

Cegid's security is managed by a centralised team that is guided by the ISO 27001 standard for the entire Group. Cegid is ISO 27001:2013[2] certified for the following areas:

- "Service enabling application hosting that contains data provided by customers in a Cloud environment"

  Certificate no. IS 666376 issued by BSI

  Sites in France: Lyon (69), Vénissieux (69), Boulogne Billancourt (92), Nantes (44)

  Cegid SaaS services concerned by this certification: Cegid Expert, Cegid Fiscalité (ex-Your Cegid Fiscalité), Cegid HR Sprint, Cegid HR Ultimate, Cegid Loop, Cegid Optitaxes, Cegid Portail Etafi, Cegid PMI, Cegid Quadra (ex-Cegid Quadra Expert), Cegid Quadra Entreprise, Cegid Retail Y2, Cegid RHP, Cegid RHPi, Cegid Talentsoft, Cegid Tax Ultimate, Cegid XRP Flex, Cegid XRP Sprint

- - "SaaS HR and Payroll services provided in different service models to facilitate HR management for Cegid Spain customers"

  Certificate no. IS 589848 issued by BSI

  Location Spain: Madrid

  Cegid SaaS services concerned by this certification: Cegid Peoplenet in Spain and Latin America

- - "Service enabling application hosting for the management and development of human resources containing data provided by customers, in a Cloud environment"

  Certificate no. CA09/77186 issued by SGS

  Canada site: Montreal

  USA site: New York

  France site: Paris (75)

  SaaS services concerned by this certification: Cegid Talent

  "Information security management system that supports SaaS (Software As A service) for time management with the Cegid VisualTime solution, in accordance with the declaration of

[2] Work on the transition to ISO 27001:2022 is underway in the various areas mentioned above.

applicability with version 2.1 and dated 24/04/2023.Certificate no. SI-0424/21 issued by LGAI Technological Center

Location Spain: Barcelona

Services covered by this certification: Cegid VisualTime

- "Design, delivery, and ongoing support of the StorIQ application"

  Certificate n°20/3244 delivered by CfA

  UK site: London

  Cegid SaaS services covered by this certification: Cegid Retail Store Excellence

  - ISAE 3402 Type II report on Cegid Tax Ultimate (France only)

  - SOC1 Type II report on Meta4 (Argentina and Mexico)

  - SOC2 Type II report on Meta4 (Spain, Portugal, Argentina, Mexico, Colombia and Chile)

  - SOC 2 Type I report on Talentsoft Career

  - ISAE 3402 Type II report on PeopleNet France

  - Certification Customer Security Program (CSP) Swift for Cegid Treasurery based on the CSCF

  The following Cegid SaaS services are covered by this Security Assurance Plan even though they are not within the scope of the previous certifications: Cegid Assurex, Cegid Digitalrecruiters, Cegid ISIE, Cegid Orli, Cegid Peoplenet in France, Cegid Retail UR, Cegid XRP Ultimate, Cegid Treasury.

  If you are unable to locate your product in the lists, do not hesitate to contact our sales department for more information.

The aim is to protect functions and information from loss, theft or alteration and to protect IT systems from intrusion or disaster.

Respecting the Secure Software Development Life Cycle allows us to guarantee a proper level of security on the hosted applications. This lifecycle is based on the principles of the OWASP SAMM, BSIMM and OWASP ASVS guidelines.

6. RISK MANAGEMENT

The Group's risk assessment process includes the identification, analysis and management of risks related to the business model and user entities.

Cegid recognises that risk management is an essential component of its business. The management has established a Cegid Cloud risk map in four areas:

The following risk types:

- Risks relating to human resources
- Strategic risks
- Information System risks
- Other risks

This process enables the Cegid management to understand and monitor relevant risks that may affect the company and to put in place measures to mitigate them.

In addition, risk analysis specific to the various ISMS are implemented based on the principles of ISO 27005 standard and internationally recognised methods (EBIOS 2010, EBIOS RM, MAGERIT, Octave, etc.).

Risk analysis is an integral part of Cegid's IS security. It is carried out continuously between the operation teams and the security teams.

7. INFORMATION SECURITY POLICY

Cegid's activities are governed by Information Security Policies. These policies have been in place since 2008 and are reviewed annually. They are based on the principles and good practices of standards ISO 27001:2013 and ISO 27002:2013.

These policies are intended to protect the critical information of Cegid, its customers and partners.

The policies are communicated to the persons concerned. To ensure the best possible protection for the security and integrity of its platforms, Cegid does not disclose the names and information relating to the security elements used (suppliers, software companies, etc.).

8. ORGANISATION OF INFORMATION SECURITY

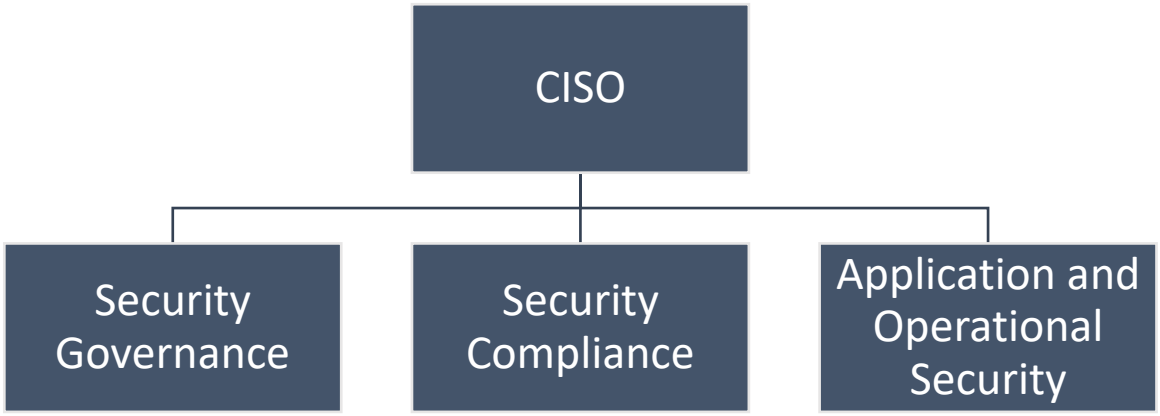
8.1. Internal organisation

8.1.1. Roles and responsibilities

Responsibilities for security have been defined and assigned.

A CISO is appointed for all Cegid activities. This person is in charge of a team dedicated to information security.

The parties involved in information security are:



8.1.2. Segregation of duties and areas of responsibility

In order to limit the risk of the unauthorised or unintentional modification or alteration of assets, the teams' tasks and areas of responsibility are segregated.

In particular, all hosting activities for our customers are segregated from the rest of the company's environments, both organisationally and technically.

In addition, within the hosting activities for our customers, a principle for the separation of tasks is implemented through rights management linked to job's needs.

A matrix organisation of the Group allows for the definition of areas of responsibility by activity, including those related to responsibility for the security of customer data and assets and risks enabling the delivery of Cloud services.

8.1.3. Governance

Governance bodies are in place at strategic level and at operational level, with dedicated committees.

These bodies meet regularly to monitor issues relating to information system security. The minutes are stored in the document management system.

8.1.4. Relationship with bodies and authorities

Cegid is a member of professional associations (CLUSIF (French information security club), CESIN (French digital information security experts club), Incibe (Spanish national cybersecurity institute), etc.), Club ISO27001. Cegid maintains relations with the authorities (ANSSI (French national information system security agency), CNIL (French data protection agency), CCN-CERT (Spanish national cryptological centre - Computer Emergency Response Team), AEPD (Spanish data protection agency), CERT-MX (Mexican Computer Emergency Response Team), etc.) in order to monitor developments in the field of information security.

8.1.5. Security monitoring

Technical and legal security monitoring is in place and carried out as part of Cegid's activity. It is used to prevent risks specifically related to Cegid's activities.

Cegid also relies on the CERT services of companies specialising in security monitoring to increase its search capabilities. This method of performing multiple searches makes it possible to cross-reference the information found and to obtain appropriate results relevant to the context of Cegid's activity.

9. HUMAN RESOURCES SECURITY

9.1. Recruitment

Applicant information is checked in accordance with the regulations, ethics, laws and any relevant legislation in force in the jurisdiction concerned. This check is proportionate to the requirements of the job, the classification of the accessible information and the identified risks.

Among the checks in place are:

- Verification of the candidate's CV;
- Verification of the skills related to the job;
- Copies of diplomas, training and professional qualifications claimed in the CV;
- Independent identity check, passport or ID card;
- Verification of the validity of the work permit, or residence permit if the candidate is an immigrant.

9.2. Confidentiality management

The following aspects are covered in the contracts, the Internal Rules and the Acceptable Use Policy:

- Respect for intellectual property;
- Compliance with personal data protection legislation;
- Protection of information, information assets, and applications of the company and its customers;
- Protection of information from partners, other organisations or third parties.

Special provisions may apply in the following situations:

- Triggering of a formal and communicated disciplinary process against employees who violate information security rules. This acts as a deterrent to employees breaching company security policies and procedures, as well as any other security rules;
- Responsibilities stipulated in the employment contract continue to apply for a defined period after the end of the contract.

All employees are contractually required to maintain confidentiality. All information provided by Customers through documents or meetings is covered by this confidentiality agreement.

9.3. Skills management

9.3.1. Security awareness

New employees follow an induction course which includes ensuring they are aware of security and confidentiality issues.

An awareness plan and specialised tools allow regular monitoring of sensitive security issues (phishing campaign, safe desk, etc.).

9.3.2. Skills and training

In order to maintain know-how, identify training needs and organise knowledge sharing, performance and objective reviews are held each year between Cegid employees and their managers. During these reviews, training plans are discussed. HR produces an annual training plan based on the expression of these needs and the company strategy.

10. ASSET MANAGEMENT

10.1. Inventory

Cegid sets up inventories of essential and supporting assets. These are listed in the risk analyses in order to centralise the associated risks.

Where technically feasible and relevant, an automated update process reconciles the inventory with the assets included in the SaaS scope.

10.2. Identification of assets

The identification of assets used in the provision of services by Cegid is based on formal naming conventions. In most cases, and where relevant, these naming conventions do not allow a direct link to customers to be made.

10.3. Document management

Cegid has implemented document management systems that take into account the processes and procedures necessary for the operation of the services provided to customers.

10.4. Management of media and hardware affecting customer data

10.4.1. Storage

Removable media containing customer data are stored in a secure location when not in use.

Non-removable media containing customer data are hosted in data centres.

10.4.2. Physical transfer

For the physical transfer of media containing non-public data, Cegid only uses recognised and reliable carriers, offering tracking and proof of delivery. Should Cegid be required to return data on media sent at the customer's initiative, it will be sent using the same techniques and means as when it arrived.

10.4.3. Scrapping

The scrapping of assets is subject to a special procedure for the deletion of confidential data. This procedure requires secure deletion or physical destruction of media that have contained confidential data.

10.4.4. Maintenance

Cegid's infrastructure providers are responsible for hardware devices containing customer data.

10.5. Management of Cegid employees' hardware assets

10.5.1. Hardware maintenance

Cegid's employee workstations are provided by the Cegid IT Department. The hardware maintenance of these machines is carried out by Cegid IT and its suppliers. An inventory is kept of the assignment of these workstations, and employees are made responsible for their physical security.

10.5.2. Scrapping

The storage media present in scrapped hardware are destroyed securely in accordance with the applicable procedures (data erasure software, deletion of disk encryption keys, etc.).

10.5.3. Removable media management

A security policy for removable media is implemented and managed for Cegid Cloud team employees. This policy is implemented by endpoint software or GPOs that do not allow the use of removable media to be restricted

10.5.4. Update, antivirus, media encryption

The IT Department is responsible for system and application updates for Cegid (office automation, internal applications), updating protection against malware and encrypting media (internal and removable). Indicators are produced regularly and analysed by the security team.

11. OPERATING SYSTEM SECURITY POLICY

A hardening policy designed to secure operating systems is implemented. The aim is to reduce the possible attack surface by deactivating or removing non-essential objects (services, applications, features, etc.). This involves setting up special security options and updating software.

11.1. Server operating system

Hardening operations on server operating systems relate to:

- Updates
- Account strategy
- User and network rights
- Logging
- Protection against malware
- Service role and functionality
- User space
- Disk space

These operations are based on the CIS (Center for Internet Security), ANSSI and NIST (National Institute of Standards and Technology) guides.

12. ACCESS CONTROL

12.1. Password policy

Each Cegid user is authenticated using a unique username and a strong password.

User passwords are not stored in clear text in the Cegid information system.

The default rule for our scopes is to use non-reversible hash-type encryption functions with secure algorithms.

For AS400 scopes, a Vigenère cipher with an X-OR key is implemented.

12.1.1. Policy for Cegid technical administrators

Password management for Cegid technical administrators is subject to a strict security policy:

- Minimum size: 10 characters.
- Complexity: upper and lower case letters, number and symbol
- Change frequency: every 60 days
- None of the last 24 passwords may be reused
- Locked after 5 attempts (unlocked by a Cegid administrator)

12.1.2. Policy for Cegid customers

The standard password policy for Cegid customer users is as follows:

- Minimum size: 8 characters.
- Complexity: upper and lower case letters, number and symbol
- Change frequency: every 90 days
- None of the last 24 passwords may be reused
- Locked after 5 attempts (unlocked by a Cegid administrator or by the user via an online password management tool)

Some applications allow the management of login information to be delegated to the Customer. When this identity federation is enabled, the Customer is free to manage and apply their own password policy. Cegid recommends that its customers use this option while respecting the requirements of the GDPR.

12.2. Access rights management

The management of access rights for the Cegid teams is based on the principle of minimum privilege. Each team has only the rights required for the activity it carries out.

Periodic access controls are performed by Cegid Security eam.

Requests for rights (addition, modification, deletion) to the main applications and domains are made via workflows.

For confidentiality reasons, no personal data relating to Cegid employees will be communicated.

12.3. Server access management

Only persons with the necessary authorisation may access servers containing customer data. Cegid has specific directories for the production scope that are separate from the internal IS.

12.4. Removal of access

The removal of access for Cegid staff is linked to the HR process for managing departures or internal mobility. These actions are monitored and tracked using internal workflow tools.

For external employees, their manager is responsible for changing or deleting their rights.

12.5. Access rights review

The review of the rights for the main scopes and applications is organised by the security team. Access reviews are carried out regularly based on a risk analysis.

13. CRYPTOGRAPHY

13.1. Data transfer to public networks

Data is encrypted when transferred to public networks using secure protocols (HTTPS, TLS, SFTP, SSH, etc.)

13.2. Data transfer to other media

In the case of removable media (e.g. USB keys or disks), the media must be encrypted by the customer and, if necessary, with the help of the support teams before being sent to Cegid. If this is not the case, the customer is responsible for the security of their data during transport and receipt at Cegid. The media, after integration of the data, are wiped before being sent back to the customer.

13.3. Certificates

In order to guarantee the best possible level of security, the HTTPS certificates used by Cegid are issued by public and recognised certification authorities. The management of these certificates is governed by procedures covering their life cycle.

13.4. Encryption

The rules for the length of the encryption keys are:

- Asymmetric encryption: greater than or equal to 2048 bits
- Symmetric encryption: greater than or equal to 256 bits

Cegid uses encryption software based on AES256 to create secure archives.

Regarding encryption, the connection protocols for our external sites are at least TLS 1.2.

13.5. Mobility

Cegid's administration teams use only their laptops to connect remotely.

14. PHYSICAL AND ENVIRONMENTAL SECURITY

14.1. Location

The data centres used by Cegid are located all over the world in order to meet the regulatory constraints of its customers. Cegid ensures that its suppliers are compliant both technically and in terms of security. The choice of data centres is made before going into production and based on the Cegid offers.

14.2. Data centres

14.2.1. Physical security of sites and access control

In order to offer an optimal level of security, the data centres used by Cegid are all ISO 27001 certified. Only authorised persons may visit the data centres.

14.2.2. Hardware security

A set of measures and principles have been applied to the infrastructure design to ensure the optimal availability and integrity of Cegid's services.

The main rule is to avoid any single point of failure (SPOF) in the hardware and network links.

For example:

- Redundancy in the physical servers
- Redundancy in the network
- At storage level
- Virtualisation

14.3. Cegid

14.3.1. Site security

The Cegid premises are subject to the same rules as the rest of the Cegid Lyon Vaise premises, mainly:

- Energy supply with individual contract + UPS
- Fire detectors, fire extinguishers
- Provision of HVAC (Heating, Ventilation, Air Conditioning) services.

14.3.2. Physical access control

Access to the premises is secured by badge readers. Each employee has a programmed badge allowing them full or partial access to certain parts of the building.

Physical access controls are part of the rights management described in paragraph 12.2.

14.3.3. Clean desk

A clean desk policy is in place at the Cegid team premises. Documents, media or any other material that may contain confidential information are stored away when not in use.

15. OPERATIONAL SECURITY

15.1. Data

15.1.1. Data classification

Standard ISO 27001 requires a classification of critical assets and information. This classification consists of at least three levels:

- Public
- Limited
- Confidential

Within this framework, customer data is classified as “Confidential”.

15.1.2. File security

The data files are stored in dedicated directories for each of our customers. These directories are protected with the security mechanisms provided by the underlying operating systems.

This ensures security, partitioning and isolation between each customer.

15.1.3. Database security

Cegid uses standard and well-known systems such as Microsoft SQL, Oracle, MySQL, MongoDB, DB2, etc. for its databases.

The selection of major players in the field allows Cegid to rely on confirmed software companies and a very active community to maintain its database management systems at an optimal level at all times.

15.1.4. Data encryption

Data is secured during transfers between the customer's workstation and the Cegid IS using encryption protocols described in 13.1.

15.1.5. Data integrity

Cegid uses procedures, technical measures and secure protocols for the transmission and storage of its customers' data in order to protect against alteration (deliberate or accidental).

15.1.6. End of contract

Details of the retention and deletion of customer data following the termination of a contract are set out in the contractual documents.

15.2. Change management

The changes follow the process described below:

Application changes:

- Standard and normal changes are authorised following validation by the committee. For example, these changes include: standard portal updates, tax updates, changes in settings, patches for bugs and vulnerabilities, etc.

Infrastructure and system changes:

- Authorised following validation by the committee: infrastructure changes with a direct impact on production, incident resolution, capacity management, security.
- Authorised without validation by the committee: routine operating actions to maintain production in operational conditions.

Special periods:

- Depending on the seasonality of our customers' products and businesses, changes are limited during certain periods, generally referred to as “freeze periods”

URGENT changes:

- Urgent changes need to be implemented quickly and cannot wait for the next validation cycle.
- This category of change is reserved for the resolution of a crisis or imminent critical risk (e.g. security breach, major incident).
- This category of change is dealt with in an emergency committee (e.g. eCAB / Emergency CAB).

15.3. Protection against malware

The entire server infrastructure is protected by centralised antivirus and anti-malware solutions. The hub servers check for updates from the software company at least once a day. They are then distributed to all servers.

Antivirus monitoring is included in the supervision of the Cegid IS and is the subject of indicators reviewed during information security committees.

15.4. Backup

15.4.1. Backup policy

Customer data is the centre of attention for the Cegid teams. In order to ensure the integrity and availability of the data, Cegid operates a high-performance backup system.

The principle adopted by Cegid is that of a double backup:

- A first backup is made from the production systems on a first dedicated infrastructure.
- Duplication is then carried out on a second dedicated infrastructure.

The backup infrastructure is not located in the same data centre as the production systems. This organisation makes it possible to guarantee an optimal level of availability and integrity while meeting our RTO and RPO requirements (see chapter 20.3).

The frequency of backups and the retention period is specific to each offer and is detailed in the Terms of Service for the offer concerned.

15.4.2. Controls and restoration

Control of the backup tasks is carried out by the reporting tools. In the event of an incident during a backup, an alert is issued automatically and processed by the Cegid teams.

As part of its regular operations, Cegid carries out restorations on a daily basis. These serve to validate the correct operation of the backups and the associated restoration processes.

15.4.3. Retention principles

As a specialised software company, Cegid knows its customers' businesses and needs well. This knowledge has allowed it to establish specific backup retention times for each offer.

The retention principles are detailed in the Terms of Service of each offer.

15.5. Log management

15.5.1. Collection of logs

Traceability on the Cegid IS is ensured using tools for the concentration and correlation of event logs. These are kept for technical and operational purposes for a period of time determined based on the legal, contractual and operational constraints.

These tools make it possible to standardise the retention period of the information collected and to guarantee its security.

The information collected is for example the user's name, the time they logged in and out, the application used, the source IP address, etc.

The logs are accessible to the Cegid teams and cannot be exported for the Customer. These logs may be provided to the Customer only upon legitimate request, such as for resolving an incident. Some Cegid offers propose application logs available directly from the application.

15.5.2. Tool access policy

The tools are accessible for Cegid Cloud employees for the specific needs of the platform's operation and with rights adapted to their functions (see chapter 12).

15.5.3. Use of logs

Examples of use of the information collected:

- To meet the regulatory and contractual constraints related to Cegid's business.
- To monitor the health of the systems managed by Cegid Cloud and be able to detect as soon as possible any event that could lead to a deterioration in the service.
- To produce anonymised statistical information about the provision of the service.

The use of statistics and information from logs is governed by the General Terms and Conditions of Use.

15.6. Supervision

15.6.1. Principles

All services and systems managed by Cegid Cloud are supervised. The supervision tools use either the SNMP protocol or specially developed PLCs to retrieve information from all control points.

A remote monitoring room allows Cegid Cloud teams to continuously monitor the health of certain services. Real-time alerts are triggered in case of malfunction for all supervised services.

The tools are combined with systems for sending SMS messages to the on-call teams during non-working hours (NWH).

15.6.2. On-call team

The on-call team is responsible for monitoring and intervening on the Cegid IS 24 hours a day, 7 days a week. It consists of specialists representing all of Cegid's areas of expertise.

15.7. Update management

15.7.1. Installed software management

Cegid uses a set of software that allows it to list and control all the software present on the IS as well as on the administration workstations.

15.7.2. System update

System updates are performed through centralised consoles.

The principle adopted by Cegid to carry out both critical and security updates is as follows: updates are rolled out on a monthly cycle on a set of test environments when a patch is released to ensure that it does not pose a problem for the integrity and/or availability of the service provided to the customers. If no problems are detected, the update is rolled out to the entire production platform.

If a patch is not available, a workaround is put in place so as not to degrade the security of the service provided.

15.7.3. Application update

Cegid is implementing an industrialised change management system (see chapter 15.2) to manage application updates in accordance with the commitments defined in the Terms of Service for its SaaS solutions.

16. SECURITY OF COMMUNICATIONS

16.1. Technical architecture

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

16.2. Telecom access

16.2.1. Internet

Cegid has its own public IP addresses as well as several Internet accesses with different providers to compensate for any failure of a provider and thus provide its customers with the expected level of service.

All communication offered by Cegid is secure and uses the protocols mentioned in chapter 13.1

16.2.2. WiFi networks

The WiFi networks are compartmentalised according to their functions (WiFi for guests, employees, mobile, etc.). Access to these networks depends on the rights management. The WiFi access points are protected.

In data centres, WiFi is prohibited.

16.3. Security equipment

16.3.1. Firewall

Firewalls are placed between each security zone and each application zone.

External flows pass through several firewall layers before reaching the requested service.

Direct flows to trusted zones are not authorised, they must pass via demilitarised zones (DMZs).

16.3.2. IDS/IPS

IDS/IPS appliances have been set up in certain strategic network locations to analyse incoming and outgoing flows from the Cegid IS. Their role is to detect abnormal flows and malicious traffic and block them.

The appliances retrieve attack signature updates from the software company's security experts and are used under the responsibility of the Cegid security team.

This data is correlated into dashboards and indicators.

16.3.3. Anti DDoS

All platforms and infrastructure benefit from anti-DDoS protection adapted to the different technologies used.

16.3.4. High availability and fault tolerance

The availability of Cegid services is ensured by the redundancy of systems to compensate for a malfunction, the failure of a component or temporary unavailability. The technologies used include:

- Server virtualisation,
- Redundancy of data storage,
- Cluster load balancing on network and telecom equipment,
- Capacity planning method with hot extending (VM and firewall),
- Application load balancing on server farms.

17. ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS

Security in developments is a major issue at Cegid.

Cegid has implemented an approach aimed at integrating security throughout the life cycle of the applications developed. This is based on the OWASP SAMM, OWASP ASVS and BSIMM recommendations.

17.1. Secure development life cycle

A governance stream includes activities related to the organisation of the secure development life cycle with the definition of policies, objectives and measures, as well as an associated training and awareness programme.

A design stream includes activities related to the collection of security requirements, high-level architecture specifications and detailed design.

An implementation stream includes activities and processes for building and deploying software components (see chapter 15.2), as well as those related to fault management.

A verification stream includes activities related to functional, non-regression and security tests that ensure the quality of the software developed.

The overall approach aims to improve the quality and security of the products delivered with, among other things:

- A community of reference developers in the security domain within each development team.
- Dedicated code security review tools
- A common reference system (OWASP) used to capitalise on security issues and ensure the dissemination and implementation of good practices.
- Specific security monitoring with information, update and improvement bulletins sent to the teams.

17.2. Partitioning of environments

Cegid's networks and infrastructure are physically and logically separated by service.

The platform also separates the different application environments (development, test, pre-production and production). The development environment is exclusively reserved for and accessible to developers, and does not include any production data unless contractually agreed with the customer.

The equipment can be accessed via an administration bastion or jump box virtual machine for teams with the necessary privileges.

17.3. Acquisition

When acquiring new systems, security needs are taken into account in the selection process.

18. RELATIONSHIP WITH SUPPLIERS

In order to produce a policy consistent with its activities, Cegid classifies its suppliers according to their criticality with regard to the provision of customer services. Depending on their criticality, different controls are put in place, for example:

- Analysis of their security certification,
- Establishment of monitoring security committees with efficiency and compliance indicators,
- Technical or organisational audits,
- Implementation and monitoring of security SLAs,
- Implementation of specific security clauses in contracts,
- Clarification of roles and responsibilities in the management of security incidents.

19. INFORMATION SECURITY VULNERABILITY AND INCIDENT MANAGEMENT

19.1. Vulnerability management

Vulnerabilities are graded according to CVSS V3.0 and processed by default in accordance with the following table:

Type of vulnerability	CVSS score	Commitment on action plan
Low	0.1 – 3.9	Best Effort
Medium	4.0 – 6.9	Best Effort
High	7.0 – 8.9	7 days from detection
Critical	9.0 - 10	7 days from detection

Some products or services may have higher commitments specified in the terms of service.

19.2. Vulnerability scanner

Scans of the entire Cegid IS Internet scope are run regularly, at least once a month, via a vulnerability scanner managed by the Cegid security team.

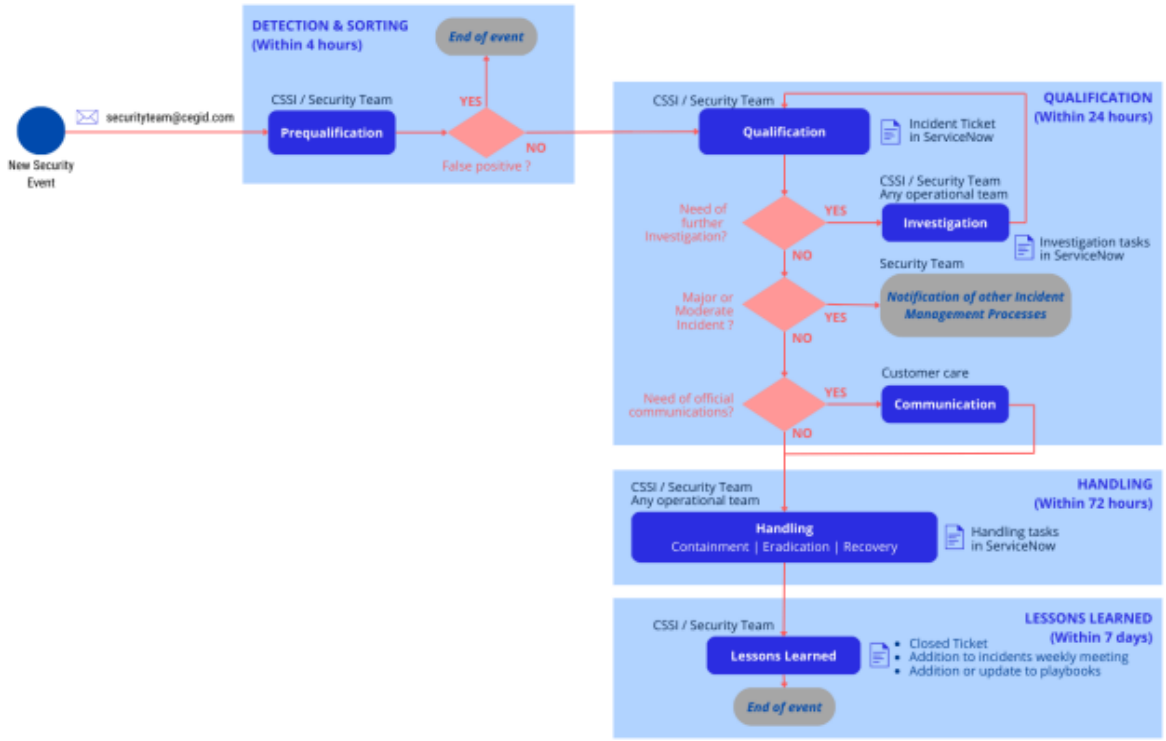
These scans are used to check the correct configuration of hardware and software in order to detect the appearance of vulnerabilities.

The results are reviewed and specific action plans are developed.

19.3. Security incident management

Security incidents are handled by a workflow in the Cegid ITSM tools. The principle is inspired by the good practices found in standards ISO 27001 and ISO 27002.

The principle is as follows:



Communication with the customers and/or partners concerned shall be within a maximum of 72 hours once the impacted scope has been evaluated.

Depending on the nature of the action plan, Cegid may also communicate with the relevant Cegid entities to organise the handling of the incident.

19.4. Crisis management

Specific crisis management plans are formalised.

Crisis scenarios are managed through an organisation and processes. A crisis management directory is maintained.

20. BUSINESS CONTINUITY MANAGEMENT

20.1. Continuity of coordination

A continuity plan is defined for the management and coordination of the services (infrastructure, applications, etc.) for Cegid teams.

The continuity of these activities is based both on the implementation of resilient architectures for the coordination systems and on the security of the laptops, allowing any Cegid team employee/administrator to have secure remote access, based on the rights granted to them, to the resources and tools used to provide the service.

20.2. BCP & Resilience

Business continuity is taken into account by default from the design phase of the services provided by Cegid.

The business continuity plan (BCP) is defined comprehensively and includes a human, organisational and technical component. It is broken down and adapted to each business offer based on the business constraints and technical architectures.

Critical resources (human resources, infrastructure, information systems, intangible resources) are identified for each business offer.

The BCP is designed to meet the continuity needs expressed in terms of service availability.

In addition to designing resilient technical and software architectures, the operational and organisational processes of the BCP are defined and tested in a continuous improvement mode.

20.3. RPO & RTO

20.3.1. RPO

RPO: Recovery Point Objective

The RPO is listed in the terms of service. By default, it is 24 hours.

20.3.2. RTO

RTO: Recovery Time Objective

As standard, Cegid does not define an RTO in the Terms of Service, but for certain specific offers, an RTO is guaranteed (see contract or terms of service).

In the event of a major disaster resulting in a sustained interruption to the service, Cegid undertakes to restore the service as soon as possible using the most suitable backup.

21. COMPLIANCE

21.1. Standards and regulations

21.1.1. ISO 27001

The Cegid teams use standard ISO 27001:2013 to design and operate the services provided to customers. The certifications and scopes covered are listed in chapter 5

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

21.1.2. GDPR and privacy

Cegid has a Privacy and cookie policy available on its website: https://www.cegid.com/en/privacy-policy/

21.1.3. Audit

21.1.3.1. Internal audit

The control of security activities within the Cegid certification scopes is carried out by qualified consultants under the supervision of the security department.

They review the elements related to the certified scopes at scheduled intervals in accordance with the Cegid audit plan.

Documents relating to internal audits are confidential and may not be disclosed. Cegid undertakes, in the event of non-compliance resulting in a breach of security, to communicate with the customer(s) concerned in the affected scope (see the Security incident management section).

21.1.3.2. External audit

As part of the certifications listed in Chapter 5, Cegid is audited annually by the certifying bodies on the scope of each of these certifications.

21.1.3.3. Technical audit

Cegid also has regular technical audits carried out on its IS by qualified experts.

These technical audits are scheduled regularly, allowing for the testing of each strategic application over a 3-year cycle

21.1.3.4. Customer audit

Subscribing customers can perform pentests on the services they use under the conditions specified in the contract.

Organisational audits can also be carried out at the customers' initiative. They are subject to certain eligibility conditions and require the signature of specific contractual clauses.