Imagicle UC Cloud Suite security.

Rel.1.1 – 19 January 2021

Contents

1 Introduction 4

2 Data center 5

3 Data Security 5

3.1 Customer Data 5

3.2 Data isolation 5

3.3 Data encryption 5

4 Log and Audit 6

5 Information Security Management System 6

6 Disaster Recovery 6

7 Imagicle Software Development Life Cycle 7

8 Security Vulnerability Responses 7

9 Imagicle Employees 8

10 Regulatory compliance & certifications 8

10.1 ISO/IEC 27001:2013 8

10.2 Governance and risk management 9

1 Introduction

This document provides an overview of Imagicle's regulatory compliance, certifications and supporting processes that are designed to protect and secure data in Imagicle Cloud.

Imagicle spa (hereafter "The Company" or "Imagicle") is committed to achieve, guarantee and maintain the principles of **Confidentiality**, **Integrity** and **Availability** and the trust of its customers.

Imagicle recognizes this is fundamental for customer's business activity.
Imagicle's priority is to form customer relationships built on trust by delivering transparency of Imagicle's operations, policies and procedures that safeguard their data.
Imagicle is committed to safeguarding and measuring its performance against and compliance with the highest security standards.
Imagicle continuously monitors current day industry threats and uses those to improve its day-to-day information security policies and procedures as an integral part of its service.

Imagicle's robust security program carefully considers data protection matters across the **Imagicle UC Cloud Suite** offered to the customers (hereafter the "Service Scope").

Imagicle UC Cloud Suite is deployed on **AWS** data centers around the globe.
All data centers are classified as ANSI/TIA-942 Tier 4, the most stringent level, designed from the ground up to host mission critical computer systems, with fully redundant subsystems and compartmentalized security.

The partnership with AWS enables Imagicle to **deploy** the UC Cloud Suite on virtual servers strategically located on **the 20+ regions around the world** to eliminate and reduce the potential of latency issues seen in some globally scaled cloud-based solutions.
Such vast geographical coverage enables Imagicle to comply with the various policies and regulatory requirements relating to handling and storing **Personally identifiable information (PII)**.

Each customer of the UC Cloud Suite has one (or more) dedicated Windows Server based on virtual machines, ensuring complete isolation of the computing, associated storage units and networking used within the customer instance.
This architecture approach provides the following benefits:

- **Security**: Complete separation ensuring isolation of all customers' data.
- **Reliability**: The performance of one customers' instance will never be impacted by activity on other Imagicle Cloud customers.
- **Proximity**: Virtual Machines instances are deployed by default in the main 3 AWS geo regions: Northern California(US), Frankfurt (Europe), London (UK), Bahrain (Middle East), with possibility to deploy on the other 20+ AWS region based on customer requirements.
- **Version Isolation**: Customers can get their cloud instance updated in agreement with Imagicle, independently from other customers.

Imagicle UC Cloud Suite has been built from the ground up in adherence with industry best practice and current day regulatory requirements, providing the **highest level of security** ensuring:

- Confidentiality
- Integrity
- Availability
- Privacy

2 Data center

Imagicle UC Cloud Suite is deployed across the AWS data centers. AWS geographical coverage enables the compliance with the various local policies and regulatory requirements regarding the handling and storing of personal and financial data ensuring the highest levels of security, reliability, transparency and compliance.
All data centers are classified as ANSI/TIA-942 Tier 4, the most stringent level, designed to host mission critical computer systems, with fully redundant subsystems and compartmentalized security.
Customers can select the most appropriate geographical location for their deployment from the data centers available from AWS.

AWS adheres to rigorous security controls which govern its operations and support.
Amazon deploy combinations of preventive, defensive, and reactive controls including the following mechanisms to help protect against unauthorized developer and/or administrative activity:

- Tight access controls on sensitive data, including a requirement for two-factor smartcard-based
- authentication to perform sensitive operations
- Combinations of controls that enhance independent detection of malicious activity
- Multiple levels of monitoring, logging, and reporting.

Additionally, AWS conducts background verification checks of certain operations personnel and limits access to applications, systems, and network infrastructure in proportion to the level of background verification.
AWS meets a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1, and SOC 2.
AWS's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate AWS services work with and meet world-class industry standards, certifications, attestations, and authorizations.
Imagicle takes advantages of its wide array of security tools and capabilities to address business objectives and industry standards and regulations.

3 Data Security

3.1 Customer Data

Customer is the exclusive owner of the Customer Data loaded on the System.
Customer has all right, title and interest in and to all of the Customer Data.
Imagicle Cloud Operation team is not allowed to access customer data except having official approval by customer authorized contacts for troubleshooting or other purposes.

3.2 Data isolation

Imagicle Cloud provides customers with a dedicated virtual machine instance(s). Each virtual machine isolates tenant operation at the OS, database and application server layer.
All software components are dedicated for each customer instance and never shared across multiple customers.

3.3 Data encryption

All data exchange can be encrypted according the choice made by customer and compliance with local architecture.

By default Imagicle will provide certificate from public CA for all HTTPS flows. For communications flows, Imagicle UC Cloud Suite support encryption by certificate (SIPs) for all provided applications. This configuration will require compatibility and configuration in customer environment.

4 Log and Audit

Any access to the Cloud environment by the Imagicle Cloud Operation team is also logged and managed via Password Access Management (PAM) tool.
Accesses by all system administrators are logged. The log files are securely stored on an AWS repository.

Only Cloud Operation Team can access Imagicle Cloud Resources.
This access is authorized via Role Based Access control and access to any Data Center server is further protected by an SSL VPN that use a personal encryption's certificate.

Every session is recorded and available for customer.

5 Information Security Management System

The company follows a specific procedure to trace, manage and monitor any security related incident or events.
The primary aim is to ensure that the best possible levels of information security and highest level of service quality and availability are maintained.

This is achieved through the following:

- The definition of adequate management structure to prepare, mitigate and respond to adverse events
- The appointment of suitable personnel to respond to incidents with the necessary responsibility, authority and competence to handle an accident and maintain the security of information
- The development and approval of documented plans, response and recovery procedures detailing how the organization has to handle an adverse event and how the security of information is maintained at a predetermined level, based on approved goals of managing information continuity
- Information Security events must be promptly notified to Information Security Manager.

In the event of a security data breach, the customer is notified. In a timely manner, a shared remediation plan is implemented to resolve the issue.

6 Disaster Recovery

Our infrastructure and Services are hosted on AWS cloud services. Imagicle services has been designed according AWS best practices including security while making every effort to ensure resilience of services based on AWS infrastructure.
The Disaster recovery plan will depend of the taken options. We have two type of DR and business continuity

- **Warm Standby (no HA Option) :** keeps a duplicate version of the organization's core elements running on standby at all times, so in a disaster, the mirror instance can be involved
- **Hot Standby (HA Option) :** replicates fully the data and applications in two or more active locations. In the event of a disaster, traffic is re-routed to the unaffected location, meaning close to no downtime.

Part of included services, data and configuration backups are stored in a dedicated area to guarantee isolation.

7 Imagicle Software Development Life Cycle

Imagicle incorporates security during the software development life cycle.
Imagicle has and follows an Agile system development methodology, composed by specific phase:

- **Analysis & Design**
  The development of the Imagicle product and its characteristics starts with the collection and analysis of requirements. The R&D team considers each feature and determines the possible threats for this feature, security by design approach. Countermeasures are put in place to prevent and mitigate each threat.
- **Development**
  To perform all releases in a secure and safe way, the R&D team follows a dedicated IT Security measures checklist. The system is protected against top 10 OWASP ‘Open Web Application Security Project’ threats, by scanning through dedicated professional tools.
- **Test**
  Test cases are created from a security perspective and executed during the development process. Testing includes system level, feature level, penetration level. Test cases consider the end-to-end new product release to identify any security issues within the new product. Specific tests are conducted on code that contains the new features within the product.

All developers and testers follow a security training program in order to improve and implement the methodologies that allow to apply security techniques aimed at minimizing the number and severity of threats.

The Imagicle R&D team follows detailed standards and techniques to make the security system work effective. Imagicle has in place a process of Vulnerability Assessment, performed continuously via state of the art market tools, to detect vulnerabilities.
Before validating a new version of the software for the UC Cloud Suite, a specific solution vulnerability assessment is run on the sandbox environment.

8 Security Vulnerability Responses

Upon identification of any security vulnerability, Imagicle can exercise commercially reasonable efforts to address the vulnerability in accordance with the following policy:

Priority	Timeframe	Version
High Risk (CVSS 8+ or industry equivalent)	60 days	Active (latest shipping one)
Medium Risk (CVSS 5-to-8 or industry equivalent)	180 days	Active (latest shipping one)
Low Risk (CVSS 0-to-5 or industry equivalent)	Best Effort	Active (latest shipping one)

Priority is established based on the current version of the Common Vulnerability Scoring System (CVSS), an open industry standard for assessing the severity of computer system security vulnerabilities. For additional information on this scoring system, refer to https://en.wikipedia.org/wiki/CVSS

Imagicle is also responsible to update and secure the **Windows Server OS** running on the Imagicle UC Cloud Suite instances.

9 Imagicle Employees

Imagicle addresses security at the initial recruitment stage. Security associated responsibilities are defined in employees' contracts and adherence is monitored throughout an individual's employment.
All employees assigned to the R&D department are obliged to sign a confidentiality (non-disclosure) agreement.
Careful attention is paid to validate the references and the appropriate level of background checks.
For Imagicle it is crucial to increase the level of expertise and to raise the awareness for ensuring that law, guidelines and procedures relating to data security are compliant with in full. Imagicle has in place various data security initiatives to ensure that all employees are qualified for and have a precise understanding of their tasks and responsibilities.
The Imagicle training contains a dedicated section detailing group security. All training content developed by HQ is focused on information security.
At Imagicle the information security awareness program is established in line with the organization's information security policies and covers general aspects such as:

- The needs to become familiar with and comply with applicable information security rules as defined in policies, regulations, contracts and agreements
- Personal accountability for one's own actions and inactions, and general responsibilities towards
- securing or protecting information belonging to the organization and external parties
- Basic information security procedures and baseline controls (such as password security, malware controls, clear desks and clear screen).

10 Regulatory compliance & certifications

10.1 ISO/IEC 27001:2013

Imagicle is working to achieve the ISO/IEC 27001 Certification for Imagicle Cloud.
Jointly published by the International Standard Organization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 is globally recognized information security standard that provides organizations with requirements for an Information Security Management System (ISMS).

The standard security model is based on three pillars: confidentiality, integrity, and availability of information assets.
Each of those covers a different aspect of providing information's security and protection.

An a**nnual audit** is conducted to validate compliance with the standard and a full certification occurs every three years.
Imagicle ISO/IEC 27001:2013 certificate will be available for customer and prospect review.
The **scope** of certification is "**the design, development and sale of Imagicle products and services including technical support**".

Overall Imagicle has demonstrated its commitment to manage in a secure way all processes related to Imagicle Cloud, e.g. Lifecycle development process, provisioning of the Imagicle

Cloud service, legal and regulatory compliance and an ongoing monitoring of security of information.

Moreover, Imagicle is developing an organization – wide Information Management System (ISMS) based on ISO 27001 Framework.
It contains policies, procedures, guidelines, work instruction and checklists for internal use and distributed to all employees.
The Information Security Manager (ISM) reviews and updates regularly the security policies.
This review assesses the availability, confidentiality and integrity of data, as well as conformance to the information security policy.

ISO 27001 is foreseen to be completed by the first half of 2021.

10.2 Governance and risk management

Imagicle performs an annual risk assessment that covers security risks. As part of this process, threats to security are identified and the risk from these threats are assessed.
The Risk Assessment phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level.
According measures, recommendations and controls are put in place to mitigate the risks to the extent possible.
As part of the overall ISMS – Information Security Management System- Framework baseline security requirements are constantly being reviewed, improved and implemented.
This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.
Each version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders.
In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.