Imagicle Security Policy

Updated on June 16th, 2023

Imagicle spa
Via Fondacci, 272
55054 Massarosa
(LU) Italy

T +39.0584.943232
F +39.0584.943325
E info@imagicle.com
W www.imagicle.com

€ 353.080,00 paid up cap.
VAT ID IT 01715870463
company reg. 01715870463

a company part of Zucchetti spa

1 Background

Imagicle is a software house specialising in software design, development, marketing and support, providing a complete set of UC applications, in a single suite, using state-of-the-art methodologies based on Agile SCRUM – Test Driven Development. The company bases its UCX Suite on standard protocols and the latest web technologies while maintaining the highest level of expertise to integrate its solutions with market leading UC platforms on-premise, hosted and in the Cloud.

With the ever-increasing use of new technologies, it is necessary to provide guarantees not only on the quality of the services provided, but also on the processing of information concerning service delivery, internal staff, agents, partners, customers and suppliers. Information is a corporate asset which, like other assets, has a value to the organisation and therefore must be protected appropriately. Security is about protecting information from a wide range of threats so as to ensure business continuity, minimise damage and maximise return on investment and business opportunities. Preserving the trust that Customers have in Imagicle requires that everyone contributes to the respect, protection and security of all confidential data and information.

2 Principles

According to the definition of the ISO 27001 standard, the security of managed information is characterised by safeguarding its confidentiality, integrity and availability.
Protecting the security of a system means:

- reducing to an acceptable value the probability that information security parameters are violated;
- promptly identifying in good time when and in which part of the system this occurs;
- limiting damage and restoring breached requirements as quickly as possible.

Supported by leadership directives, Imagicle's security program directly involves teams dedicated to implementing security controls in all areas of the company, spanning a secure development lifecycle from product design to ongoing operational support. The security program is applied, monitored, maintained, improved and documented consistent with the purpose of the business and by reference to the international standard ISO/IEC 27001:2017, with the ongoing goal of reducing risk levels.

3 Objectives

The Information Security Management System (ISMS), designed by Imagicle, is based on:

- management of information security risks in synergy with the overall corporate risk management and in compliance with the responsible use of corporate resources, achieved through the application of shared, repeatable and valid models, referable to recognised international standards;

- identification of organisational roles and responsibilities specifically involved in managing information security;
- raising staff awareness on information security, training and enhancing the skills of greatest interest for information security;
- continuous monitoring of the effectiveness and efficiency of the ISMS through the definition of a system of indicators and their periodic measurement;
- commitment of the Management to provide the resources deemed necessary for the implementation of corporate security policies, the pursuit of security objectives, the maintenance and continuous improvement of the ISMS.

Imagicle equipment is designed with safety in mind, with ongoing periodic maintenance. The product development lifecycle includes product evaluations and security design reviews as standard practice within the development process. To ensure confidentiality of information, Imagicle manages both internal and external communications using appropriate encryption algorithms and certificates. Up-to-date IT and OT security tools and methods are applied throughout the product lifecycle to reduce risks and address vulnerabilities in proportion to company needs and in compliance with relevant regulations. The company's security system is aligned with international best-practices and standards, and geared towards the ISO-27001 standard, which includes implementing and enforcing strict information access control measures on a business-related need-to-know basis, and regular monitoring and testing of the ISMS.

4 References to regulatory aspects

All relevant mandatory and contractual requirements are identified by the organisation. The Regulatory Updates Procedure describes the activities to ensure that:

- regulatory updates relating to privacy (GDPR – EU Regulation 2016/679), are available and known to the various corporate functions concerned;
- the necessary updates are made to the company's operating procedures and IT systems in order to comply with the regulations in force (Compliance).

The ISMS Coordinator ensures the monitoring and approval of the application of regulatory updates in the company.

5 Diffusion of security culture and policies

Security is a capillary process that concerns the whole company: individual awareness combined with a responsible use of resources plays a fundamental role in achieving the forset security objectives. Imagicle personnel are constantly made responsible for distributing within the company a culture of information security, considered necessary for the type of services offered and data processed. This commitment involves first most the top management, providing for the definition of roles and responsibilities and keeping awareness, culture and security alive throughout the organisation. Imagicle personnel are involved through the definition of comprehensive and easy-to-understand policies and procedures on data security,

thanks to the presence of dedicated teams committed to IT and product security.
Employees and third parties involved in company processes collaborate, as far as their competence is concerned, by respecting the rules and operating procedures reported in the Information Security Management System documentation (available on the company intranet) and by applying best practices and behaviours. For this reason, communication of the company's security policies is extended to its partners, suppliers and customers at the time of signing or periodically renewing the contract.

6 Leadership commitment

The Company Management favours the development of the corporate culture towards the application of the rules and requirements of information security (as a guarantee to the company, customers, third parties) and the awareness and involvement of all functions in contributing to the pursuit of security objectives. It also undertakes to provide the resources deemed necessary for the implementation of corporate security policies, the pursuit of the relevant objectives and the maintenance and continuous improvement of the Information Security Management System, providing for the review of such policies at least once a year or in the event of significant changes in business or infrastructure.
The Company Management is committed to spreading and maintaining awareness, culture and corporate security policies to all internal and external personnel through various internal communication channels.

7 Risk analysis and management methodology

Security is continuously monitored, which is why Imagicle has adopted both an information security risk analysis and management methodology and a periodic (annual or when a change is made or a new application is implemented) risk management process to keep risks at an acceptable level by assessing and treating them. For this purpose, the following have been defined:

- the criteria for assessing and accepting risk, and objectively and transparently identifying the potential threats and vulnerabilities that may arise from the design, implementation and management of systems and that could be exploited to compromise information security;
- the related direct and indirect damages;
- the protection measures in place, so as to highlight the most critical areas and provide for the implementation of appropriate countermeasures.


imagicle®
Your Communications, easier