CASINO
ST. MORITZ

ISMS Policy CSMAG

Initial situation and scope

Casino St. Moritz AG (CSMAG) is certified in accordance with ISO standard 27001:2013 and is committed to meeting these requirements. The scope of the certification covers all online gaming business activities and processes (including the implementation of the GWG and social concept) at all locations and for all employees and services.

Information security objectives

CSMAG has set itself the following goals:

- Adequate protection of information in terms of availability, confidentiality and integrity.
- Fulfilment of legal, contractual and internal requirements in the area of information security.
- Use ISO 27001 as an everyday tool for information security and constant further development.

The ISMS of CSMAG

CSMAG's information security management system documents all procedures and rules that serve to ensure CSMAG's information security vis-à-vis its stakeholders. The ISMS is communicated on an ongoing basis and training is provided at the appropriate level. The application of these rules is mandatory and binding.

Continuous improvement

CSMAG's ISMS is continuously reviewed and adapted to current conditions. In the spirit of continuous improvement, the competences of all involved units are constantly being further developed.

Organisation and responsibilities

Management

The management is the company's highest operational decision-making body and delegates tasks, responsibilities and competences in information security to the CISO.

Internal employees / General

All CSMAG employees who perform activities within the scope of the ISMS are responsible for information security in their area of expertise. Superiors at all hierarchical levels are obliged to provide the necessary resources and skills. They are obliged to sustainably implement all necessary security measures within the scope of their area of responsibility. They shall instruct their employees and train them as required.

CISO

The CISO is responsible for the development and definition, monitoring, control and operation and continuous improvement of the ISMS. He reports to the Executive Board.

Asset Owner

Asset owners establish, document and apply rules for the permissible use of information and values allocated to them.

Risk Owner

Risk owners lead the information security risk assessment and treatment process for their assigned risks. They analyse and assess the risks and define appropriate measures.

Supplier Manager

Supplier managers manage their assigned suppliers and ensure the implementation of information security in the supply chain.

External employees / employees of third parties

The regulations of CSMAG in the context of information security apply accordingly to persons who perform activities as external parties or employees of third parties within the scope of the ISMS and must be complied with by them.

Controls

CSMAG checks information security at planned and regular intervals with internal and external audits. The results of these checks are incorporated into continuous improvement.

Sanctions

CSMAG agrees on contractual penalties with third parties, which can be claimed in the event of repeated or individual serious violations of the safety regulations and instructions. In such cases, the sanctions under labour law apply to internal employees.

Definitions of terms

Information security

Information security is understood to mean all measures that are ordered, implemented, checked and continuously improved to maintain the confidentiality, integrity and availability of information. These measures can be of an organisational, technical or structural nature, among others.

- Confidentiality: ensuring access to information only for those authorised to access it.
- Integrity: Ensuring the integrity and completeness of information and its processing methods.
- Availability: Ensuring on-demand access to information and associated assets for authorised users.

Information Security Management System (ISMS)

An ISMS is understood to mean:

- All rules, procedures and processes within the scope that define, control, implement, review, maintain and continuously improve information security.
- The documentation is carried out by means of the ISMS framework, the controls of the SOA (declaration of applicability) and with corresponding policies, process overviews and other verification documents.

CISO (Chief Information Security Officer)

The CISO is responsible for information security in his or her assigned scope.