ISMS Policy

Ausgangslage und Geltungsbereich

Die CASINO INTERLAKEN AG (CIAG) zertifiziert sich nach der ISO Norm 27001:2013 und verpflichtet sich zur Erfüllung dieser Anforderungen. Dabei umfasst der Geltungsbereich der Zertifizierung den ganzen Bereich des Online Gaming (sämtliche Mitarbeitende, Standorte, Geschäftstätigkeiten, Prozesse, Services etc.)

Ziele der Informationssicherheit

Die CIAG hat sich folgende strategische Ziele gesetzt:

- Angemessener Schutz von Informationen in Bezug auf Verfügbarkeit, Vertraulichkeit sowie Integrität.
- Erfüllung der gesetzlichen, vertraglichen und internen Vorgaben im Bereich Informationssicherheit.
- ISO 27001 als Alltagswerkzeug zur Qualitätssicherung und konstanten Weiterentwicklung der Firma nutzen.

Das ISMS von Starvegas by Casino Interlaken

Im Informationssicherheits-Managementsystem der CIAG werden alle Verfahren und Regeln dokumentiert, welche dazu dienen, die Informationssicherheit der CIAG gegenüber ihren Anspruchsgruppen zu gewährleisten. Das ISMS wird laufend kommuniziert und stufengerecht geschult. Die Anwendung dieser Regelungen ist zwingend und verbindlich.

Kontinuierliche Verbesserung

Das ISMS der CIAG wird laufend überprüft und den aktuellen Gegebenheiten angepasst. Im Sinn einer kontinuierlichen Verbesserung werden die Kompetenzen aller beteiligten Stellen laufend weiterentwickelt.

Organisation und Verantwortlichkeiten

Geschäftsleitung

Die Geschäftsleitung ist Auftraggeberin des Sicherheitsverantwortlichen. Die Strategie und die strategischen Ziele werden durch sie definiert.

CISO (Chief Information Security Officer)

Der CISO verantwortet, überwacht und verbessert das ISMS, setzt die definierten Ziele um und rapportiert zu Händen der Geschäftsleitung. Der CISO zeichnet sich verantwortlich für die Informationssicherheit in seinem zugewiesenen Geltungsbereich. Aufgrund der Unternehmensgrösse ist der CISO in Personalunion auch der Compliance Officer (CO) ISMS.

Interne Mitarbeitende / Generell

Die Mitarbeitende sind verantwortlich für die Einhaltung der Informationssicherheit. Unterstützt und geschult werden sie durch den CISO.

Externe Mitarbeitende / Mitarbeitende von Dritten

Die Regelungen der CIAG im Kontext Informationssicherheit gelten entsprechend auf für Personen, welche als Externe oder Mitarbeitende von Dritten im Geltungsbereich des ISMS Tätigkeiten verrichten und sind durch diese einzuhalten.

Kontrollen

Die CIAG überprüft die Informationssicherheit in geplanten und regelmässigen Abständen mit internen und externen Audits. Die Ergebnisse dieser Kontrollen fliessen in die kontinuierliche Verbesserung ein.

Sanktionen

Verstösse gegen die Vorgaben betreffend Informationssicherheit werden nicht geduldet und werden geahndet. Die CIAG vereinbart mit Dritten Konventionalstrafen, welche bei wiederholten oder einzelnen schwerwiegenden Verstössen gegen die Sicherheitsvorschriften und –Weisungen eingefordert werden können. Bei den internen Mitarbeitenden kommen in solchen Fällen die arbeitsrechtlichen Sanktionen zur Anwendung.

Begriffsdefinitionen

Informationssicherheit

Unter der Informationssicherheit werden alle Massnahmen verstanden, die zur Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen angeordnet, durchgeführt, überprüft und kontinuierlich verbessert werden. Diese Massnahmen können u. a. organisatorischer, technischer oder baulicher Natur sein.

- **Vertraulichkeit**: Gewährleistung des Zugangs zu Informationen nur für die Zugangsberechtigten.
- **Integrität**: Sicherstellen der Unversehrtheit und Vollständigkeit von Informationen und deren Verarbeitungsmethoden.
- **Verfügbarkeit**: Gewährleistung des bedarfsorientierten Zugangs zu Informationen und den zugehörigen Werten für berechtigte Benutzer.

Informationssicherheits-Managementsystem (ISMS)

Unter einem ISMS wird verstanden:

- Sämtliche Regeln, Verfahren und Prozesse innerhalb des Anwendungsbereichs, welche die Informationssicherheit definieren, steuern, durchführen, überprüfen, aufrechterhalten und kontinuierlich verbessern.

- Die Dokumentation erfolgt mittels ISMS Framework, den Controls der SoA (Anwendbarkeitserklärung) und mit entsprechenden Policies, Prozessübersichten und weiteren Nachweisdokumenten.