Informationssicherheits-Managementsystem (ISMS)-Politik

1 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.)

2 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.

3 Das ISMS der CIAG

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.

4 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.

5 Organisation und Verantwortlichkeiten

5.1 CEO

Der CEO ist das oberste operative Entscheidungsorgan der Firma und delegiert Aufgaben, Verantwortung und Kompetenzen für das Online Gaming Geschäftsfeld an den COO.

5.2 COO Online Gaming

Der COO Online Gaming ist gesamtverantwortlich für das Online Gaming Geschäftsfeld Starvegas bei Casino Interlaken und damit auch für die Umsetzung der Informationssicherheit. Er delegiert Aufgaben, Kompetenzen und Verantwortung in der Informationssicherheit an den CISO.

5.3 CISO

Der CISO ist verantwortlich für die Erarbeitung und Definition, Überwachung, Steuerung und Betrieb und kontinuierliche Verbesserung des ISMS. Er regelt für den zulässigen Gebrauch von ihm zugeteilten Informationen und Werte, dokumentiert und wendet sie an. Er beurteilt die Informationssicherheit und behandelt diese. Er analysiert und bewertet die Risiken, legt Massnahmen fest. Er rapportiert an den COO Online Gaming.

5.4 Interne Mitarbeitende / generell

Alle Mitarbeitenden der CIAG, welche Tätigkeiten im Geltungsbereich des ISMS verrichten sind für die Informationssicherheit in ihrem Fachbereich verantwortlich. Die Vorgesetzten aller Hierarchiestufen sind verpflichtet, die dafür nötigen Ressourcen und Skills zur Verfügung zu stellen. Sie sind verpflichtet, sämtliche notwendigen Sicherheitsmassnahmen im Rahmen ihres Verantwortungsbereiches nachhaltig umzusetzen. Sie leiten ihre Mitarbeitenden an und schulen sie bedarfsgerecht.

5.5 Asset Owner

Asset Owner legen Regeln für den zulässigen Gebrauch von ihnen zugeteilten Informationen und Werten fest, dokumentieren diese und wenden sie an.

5.6 Risk Owner

Risk Owner führen den Prozess zur Informationssicherheitsrisikobeurteilung und –Behandlung für ihre zugeteilten Risiken. Sie analysieren und bewerten die Risiken und legen entsprechende Massnahmen fest.

5.7 Human Resource

Die Mitarbeitenden der Abteilung Human Resource der Congress Centre Kursaal Interlaken AG sind zuständig für die Personalprozesse von Starvegas.

5.8 Accounting

Die Mitarbeitenden der Abteilung Accounting der Congress Centre Kursaal Interlaken AG sind zuständig für die Accounting Prozesse von Starvegas.

5.9 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. Je nach Informationssicherheit sind diese verpflichtend eine Vertraulichkeitsvereinbarung einzugehen.

6 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.

7 Sanktionen

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.

8 Begriffsdefinitionen

8.1 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.

8.2 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.