Informationssicherheitspolitik

Klassifikation: ÖFFENTLICH

Dokumentverantwortlicher: Beatrice Dietrichsteiner

Geprüft und Freigegeben (somit gültig) per: 03.11.2023

Geprüft und Freigegeben von: Matthias Zwittag

DokumentNr.	Version	Aktualisiert am
DOC_26	1.1	28.06.2023

Kontaktdaten vom Dokumentverantwortlichen

SIWA Online GmbH
Beatrice Dietrichsteiner
b.dietrichsteiner@siwa.at
+43 7236 3351 4177

1. Anwendungsbereich

Der Anwendungsbereich dieser Informationssicherheitspolitik umfasst die SIWA Online GmbH mit all ihren Werten, Mitarbeiter*innen und Leistungen.

2. Zielsetzung

Der Schutz sensibler Informationen ist für die Reputation und Leistungsfähigkeit der SIWA von höchster Bedeutung.

Um dieser Bedeutung gerecht zu werden, hat die SIWA ein ISMS gemäß ISO 27001 eingeführt. Dieses wird mit dem Ziel betrieben, durch klare Vorgaben und Richtlinien sowie der Setzung von Maßnahmen, Sicherheitsrisiken für die Daten, Informationen und den damit verbundenen Vermögenswerten in den Geschäftsprozessen zu minimieren, gegebenenfalls vorhandene Sicherheitsrisiken zu identifizieren und allenfalls zu eliminieren.

Dadurch wird im Hinblick auf Informationsschutz, Schutz der personenbezogenen Daten und Sicherung der Geschäftsprozesse neben dem Nutzen für Kunden sowie Mitarbeiter*Innen auch die Zuverlässigkeit und Transparenz des Betriebes sichergestellt und dokumentiert.

Ziel des ISMS ist eine Sicherheitsstrategie, welche über das sicherheitsbewusste Handeln hinaus geht.

3. Grundsätze

Das ISMS wurde anhand der Vorgaben und Empfehlungen der Norm ISO 27001 aufgebaut und wird kontinuierlich weiterentwickelt. Beim Aufbau wurden die nachfolgenden Prinzipien angewendet.

3.1 ISMS Prozess

Es ist Aufgabe des Chief Information Security Officer (im Folgenden kurz "CISO", als „Prozesseigner ISMS“), die notwendigen Rahmenbedingungen zu schaffen und gemeinsam mit dem Top Management als Verantwortlichen dafür zu sorgen, dass der ISMS-Prozess sauber aufgesetzt und in der Organisation verankert ist.

3.2 Transparenz und Nachvollziehbarkeit

Handlungen, Maßnahmen und Entscheidungen im Rahmen des Informationssicherheits- und Risikomanagementprozesses sind aus der im Unternehmen vorhandenen aktüll gültigen Informationssicherheits Policy nachvollziehbar und ableitbar.

3.3 Need-to-know-Prinzip

Die SIWA verpflichtet sich, ihren Mitarbeiter*Innen alle Assets und Informationen zugänglich zu machen, die sie für ihre Arbeit benötigen.

3.4 Least-Privilege-Prinzip

Um ihre Assets (Daten, Systeme, Informationen, etc.) zu schützen, ist die SIWA berechtigt, alle über das Need-to-know Prinzip hinausgehenden Zugriffe auf jene Mitarbeiter*Innen zu beschränken, die den Zugriff für die Erfüllung ihrer operativen Aufgaben benötigen.

3.5 Seggregation of Duties

Um Fehler und Manipulationen Einzelner schon im Ansatz zu verhindern, sind miteinander unvereinbare Funktionen, Rollen und Verantwortungen zu trennen. Ziel ist es zu verhindern, dass sich jemand selbst kontrolliert. Ist das aus irgendeinem Grund nicht möglich, müssen kompensierende Kontrollen (z.B. regelmäßige Kontrolle der Nutzung von Administrationszugängen) zwingend eingeführt und von den Leitungsorganen genehmigt werden.

3.6 Angemessenheit

Die SIWA ist sich im Klaren, dass eine absolute Sicherheit nicht zu gewährleisten ist. Deshalb wird ein angemessenes Sicherheitsniveau (Stand der Technik) angestrebt. Daher sind die umzusetzenden Schutzmaßnahmen entsprechend der Kosten im Verhältnis zum Schutzbedarf anzupassen und ggf. Abweichungen im Rahmen des IS-Risikomanagementprozesses zu bewerten.

4. Kultur

Die SIWA bekennt sich auch im Bereich Informationssicherheit zu einer Kultur des Vertraüns gegenüber dem Wissen und Können seiner Mitarbeiter*Innen. Außerdem vertraut SIWA darauf, dass ihre Mitarbeiter*innen eigenverantwortlich handeln und sich ihrer Rolle im Bereich der Informationssicherheit bewusst sind. Dennoch sind Verstöße gegen Richtlinien und Vorgaben klar geregelt und umfassen unter anderem definierte Maßnahmen disziplinarischer Art. Weiters setzt SIWA auf eine regelmäßige Sensibilisierung ihrer Mitarbeiter*innen durch z.b.: Awareness Schulungen.

Zudem setzt die SIWA auf eine offene und lösungsorientierte Fehlerkultur. Fehler sind Chancen zur ständigen Verbesserung und sind ein fester Bestandteil des Lernens und der Weiterentwicklung.

5. Anforderungen an die Informationssicherheit

5.1 Clear Desk

Jeder muss sich an die IT-Richtlinie halten. Dies gilt unabhängig von Position, Aufgabe oder Arbeitsumgebung. Die IT-Richtlinie gilt daher auch für Homeoffice und Telearbeitsplätze.

5.2 Sicherer Datenaustausch

Voraussetzung für den Austausch von Daten und Informationen mit externen Parteien, die als "vertraulich" oder höher eingestuft sind, ist eine von allen beteiligten Parteien unterzeichnete Geheimhaltungsvereinbarung (NDA), in der die Empfänger und potenziellen Unterauftragnehmer genannt werden. Der Datenaustausch muss immer auf einer Need-to-know-Basis erfolgen.

Kategorie der Daten	**Versand per**
Logindaten	One Time Message (OTM)
Projektdaten	SIWA Fileshare

Für die Aussendung der Zugänge zu den entsprechenden Fileshares, etc. ist der jeweilige Projektmanager zuständig.

Datenaustausch per E-Mail ist nur zulässig, wenn es ein sicherer Mailservice ist (TLS/SSL…). Als "vertraulich" oder höher eingestufte Daten dürfen nicht per E-Mail versendet werden.

Nähere Infos zum Umgang mit klassifizierten Unternehmensinformationen sind in der Klassifikation von Informationswerten Policy enthalten.

6. Verbindlichkeitserklärung

Die Informationssicherheitspolitik ist ein wesentlicher Bestandteil zum Erreichen der Unternehmensziele und zur Umsetzung der festgelegten ISMS-Strategie. Die Informationssicherheitspolitik ist für alle Beschäftigten sowie relevante Dritte verbindlich einzuhalten.

7. Kontakt

Für jegliche Fragen zur Informationssicherheit steht Ihnen der CISO (Chief Information Security Officer) der SIWA Online GmbH zur Verfügung

Beatrice Dietrichsteiner
b.dietrichsteiner@siwa.at
07236/3351-4177