
	PE05-1 POLITIK DES INFORMATIONSSICHERHEITSMANAGEMENT SYSTEMS	
	Version: 2.0	Modifikationsdatum: 4/11/2024 Klassifizierung: Öffentlich

## POLITIK DES

## INFORMATIONSSICHERHEITSMANAGEMENTSYSTEMS

Durchgeführt von	Geprüft und genehmigt von
Leiter der Sicherheitsabteilung	Adresse

REVISIONEN			
DATUM	DONE	ANGENOMMEN	Beschreibung der Änderung
4/11/2024	R. Sicherheit	Adresse	Update

	PE05-1 POLITIK DES INFORMATIONSSICHERHEITSMANAGEMENT SYSTEMS	
	Version: 2.0	Modifikationsdatum: 4/11/2024 Klassifizierung: Öffentlich

Seabery, ein führender Anbieter von Augmented-Reality-Lösungen für die Schweißerausbildung, ist sich der kritischen Bedeutung der Informationssicherheit in allen seinen Entwicklungs-, Produktions- und Kundendienstprozessen bewusst.

Der Geltungsbereich unseres ISMS deckt alle Prozesse ab, die mit der Entwicklung, der Produktion und dem Support unserer Schweißsimulationen zusammenhängen, einschließlich unserer zentralen Einrichtungen und kritischen Informationssysteme.

Wir verpflichten uns, regelmäßige Risikobewertungen durchzuführen und angemessene Sicherheitskontrollen einzuführen, um unsere kritischen Informationsbestände zu schützen.

Seabery ist sich der sozialen Verantwortung bewusst, die mit der Entwicklung seiner Wirtschaftstätigkeit einhergeht, und hat eine Form des Managements eingeführt, die ein transparentes und moralisches Verhalten gegenüber seinen Stakeholdern beinhaltet. Zu den Zielen des Unternehmens gehören neben der wirtschaftlichen Wettbewerbsfähigkeit und der Erzielung von Gewinnen auch die Förderung des sozialen und ökologischen Umfelds, wofür eine Politik zur Verbesserung der Arbeitsbedingungen, der Achtung der Menschenrechte und des ethischen Verhaltens gegenüber allen Stakeholdern (Mitarbeiter, Kunden, Lieferanten usw.) verfolgt wird.

Aus diesem Grund hat sie ein **Managementsystem für Informationssicherheit** eingeführt, um die Informationsressourcen vor internen oder externen, absichtlichen oder zufälligen Bedrohungen zu schützen und die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu gewährleisten.


Die Wirksamkeit und Anwendung des **Managementsystems für die Informationssicherheit** unterliegt der direkten Verantwortung des **Informationssicherheitsausschusses**, der für die Genehmigung, Verbreitung und Einhaltung dieses Sicherheitsplans zuständig ist. In seinem Namen und in seinem Auftrag wurde ein Beauftragter für das Managementsystem für Informationssicherheit ernannt, der über ausreichende Befugnisse verfügt, um eine aktive Rolle im Managementsystem für Informationssicherheit zu spielen und dessen Umsetzung, Entwicklung und Pflege zu überwachen.

Der Informationssicherheitsausschuss entwickelt und genehmigt die im Informationssicherheitsmanagementsystem verwendete Risikoanalysemethode.

Jede Person, deren Tätigkeit direkt oder indirekt von den Anforderungen des Informationssicherheitsmanagementsystems betroffen sein kann, ist verpflichtet, den Sicherheitsplan strikt einzuhalten.

Aus all diesen Gründen verpflichten wir uns zur Informationssicherheit gemäß der Referenznorm ISO/IEC 27001, für die die Geschäftsleitung die folgenden Grundsätze festlegt:

- Managementkompetenz und Führung als Verpflichtung zur Entwicklung des Informationssicherheitssystems.

	PE05-1 POLITIK DES INFORMATIONSSICHERHEITSMANAGEMENT SYSTEMS	
	Version: 2.0	Modifikationsdatum: 4/11/2024 Klassifizierung: Öffentlich

- Ermittlung der internen und externen Interessengruppen, die am Informationssystem beteiligt sind, und Erfüllung ihrer Anforderungen.
- Verstehen des Kontextes der Seabery und Erkennen von Chancen und Risiken in der Seabery als Grundlage für die Aktionsplanung, um diese anzugehen, zu übernehmen oder zu bewältigen.
- Einhaltung der geltenden Rechtsvorschriften zur Informationssicherheit.
- Gewährleistung der Vertraulichkeit der von Seabery verwalteten Daten und der Verfügbarkeit der Informationssysteme, sowohl bei den den Kunden angebotenen Dienstleistungen als auch bei der internen Verwaltung, wobei unzulässige Änderungen der Informationen zu vermeiden sind.
- Sicherstellung der Fähigkeit, auf Notfallsituationen zu reagieren und das Funktionieren kritischer Dienste so schnell wie möglich wiederherzustellen.
- Festlegung geeigneter Maßnahmen für die Behandlung von Risiken, die sich aus der Identifizierung und Bewertung von Vermögenswerten ergeben.
- Förderung des Bewusstseins für die Informationssicherheit und der Ausbildung.
- Festlegung von Zielen und Vorgaben, die auf die Bewertung der Leistung im Bereich der Informationssicherheit sowie auf die kontinuierliche Verbesserung unserer Aktivitäten ausgerichtet sind, geregelt im Managementsystem, das diese Politik entwickelt.
- Gewährleistung des Schutzes der Privatsphäre personenbezogener Daten unter Einhaltung der geltenden Vorschriften und der Erwartungen der Interessengruppen.
- Kontinuierliche Stärkung unserer Cybersicherheitskapazitäten, um neuen Bedrohungen im digitalen Umfeld zu begegnen.
- Ausweitung der Grundsätze der Informationssicherheit auf unsere Lieferkette, um sicherzustellen, dass unsere Lieferanten und Geschäftspartner die entsprechenden Standards erfüllen.
- Entwicklung und Aufrechterhaltung der Widerstandsfähigkeit unserer Informationssysteme, um die Kontinuität kritischer Vorgänge angesichts von Sicherheitsvorfällen zu gewährleisten.

Diese Grundsätze werden von der Geschäftsleitung übernommen, die über die notwendigen Mittel verfügt und ihre Mitarbeiter mit ausreichenden Ressourcen ausstattet, um sie einzuhalten, und sie werden in dieser Informationssicherheitspolitik dargelegt und veröffentlicht.

Jeder Seabery-Mitarbeiter ist dafür verantwortlich, diese Politik zu befolgen und bei seiner täglichen Arbeit aktiv zur Informationssicherheit beizutragen.

Gezeichnet: Die

Direktion Datum:

4.11.2024