Informationssicherheitsrichtlinie

MOTIVATION

Der Mangel an Kontrolle von Unternehmen darüber, wie Daten und Informationen erzeugt, wo sie gespeichert und an wen sie übermittelt werden, birgt das Risiko von Sicherheits- und Compliance-Vorfällen, die sich negativ auf das Geschäft selbst auswirken können. Informationssicherheit ist tatsächlich ein wesentlicher Vermögenswert des Unternehmens, und die Umsetzung wirksamer Maßnahmen kann eine Strategie darstellen, die sich mit der Zeit in einen Wettbewerbsvorteil verwandelt.

Aus diesem Grund war Artificialy SA, spezialisiert auf Lösungen der künstlichen Intelligenz, stets führend im Bereich des Informationsschutzes und der Informationssicherheit. Eine grundlegende Maßnahme in diesem Zusammenhang war die Einführung eines Informationssicherheits-Managementsystems, einer Gesamtheit organisatorischer, technischer und verfahrensbezogener Prozesse, die auf bewährten Verfahren und Referenzstandards basieren, auch in Übereinstimmung mit den Richtlinien und dem internationalen Standard ISO/IEC 27001:2022.

ZIELE

Das Ziel des Informationssicherheits-Managementsystems von Artificialy SA ist es, ein angemessenes Schutz- und Sicherheitsniveau für den Informationsfluss innerhalb der Organisation zu gewährleisten, um die Konzeption, Entwicklung und Bereitstellung der Unternehmensdienstleistungen bestmöglich durchzuführen.

Ohne Verfahren zur Identifizierung, Bewertung und Analyse von Risiken könnten die Sicherheitsbedrohungen, denen die Dienstleistungen und Verfahren des Unternehmens täglich ausgesetzt sind, deren ordnungsgemäße Funktionsweise beeinträchtigen, mit möglichen wirtschaftlichen Folgen.

Die Gesamtheit der organisatorischen, technischen und verfahrensbezogenen Maßnahmen, die vom Informationssicherheits-Managementsystem von Artificialy SA festgelegt wurden, erfüllt die folgenden grundlegenden Sicherheitsanforderungen:

- **Vertraulichkeit**: Der Zugang zu Informationen wird nur denjenigen gestattet, die über die entsprechenden Berechtigungen verfügen.
- **Integrität**: Die Verwaltung von Informationen (einschließlich ihrer Änderung) unterliegt präzisen, von der Unternehmensführung festgelegten Vorgaben.
- **Verfügbarkeit**: Autorisierte Benutzer können jederzeit, wenn sie sie im Rahmen der betrieblichen Prozesse benötigen, frei auf Informationen zugreifen, wobei der Abruf schnell und intuitiv erfolgt.

Artificialy SA möchte sich im Bereich der Informationssicherheit positionieren als:

- Ein zuverlässiger und kompetenter Anbieter bei der Bewahrung des Unternehmensimages.
- Ein Knotenpunkt, an dem die Informationswerte des Unternehmens gespeichert, bewahrt und geschützt werden.
- Ein Förderer der Geschäftskontinuität für betriebliche Prozesse.
- Ein Instrument, das vollständig mit den geltenden und verbindlichen Vorschriften übereinstimmt, was zu einem Ausbau der Kompetenz des Unternehmens im Bereich der Informationssicherheit führt.

INHALT DER RICHTLINIE

Jede für die Durchführung interner Tätigkeiten notwendige Information, von Produkt-/Dienstleistungsdaten bis zu deren Konfiguration, muss während ihres gesamten Lebenszyklus geschützt werden, von der Erstellung über die Nutzung bis hin zur endgültigen Entsorgung. Das Informationssicherheits-Managementsystem ist Teil dieses Prozesses und ermöglicht eine sichere, genaue und zuverlässige Informationsverwaltung sowie einen zeitnahen Informationsabruf.

Gemäß dem geltenden Standard ISO/IEC 27001:2022 gehört zu den vom Informationssicherheits-Managementsystem geforderten Präventivmaßnahmen die verpflichtende Bewertung von Sicherheitsrisiken und deren potenziellen Auswirkungen auf das Unternehmen, die regelmäßig vom Informationssicherheitsbeauftragten durchzuführen ist. Der Informationssicherheitsbeauftragte muss überprüfen, ob die oben genannten Sicherheitsanforderungen erfüllt werden, die kritischen Faktoren analysieren, die zu Sicherheitsvorfällen geführt haben, und diese in den breiteren Kontext bereits umgesetzter oder noch umzusetzender strategischer, geschäftlicher und technologischer Veränderungen einordnen.

Der Zweck dieser Analyse besteht darin, das mit jedem zu schützenden Vermögenswert verbundene Risiko im Hinblick auf die identifizierten Bedrohungen zu bewerten. Das vom Informationssicherheitsbeauftragten für diese Bewertung angewandte Verfahren wird mit der Geschäftsleitung abgestimmt, die das Dokument, das die anzuwendende Methodik beschreibt, genehmigen muss. Darüber hinaus trägt die Geschäftsleitung auch dazu bei, die zur Bestimmung des Risikoniveaus verwendeten Parameter festzulegen. Nach Abschluss der Bewertung durch den Informationssicherheitsbeauftragten werden die Ergebnisse gemeinsam mit der Geschäftsleitung überprüft, die entscheidet, ob das Risikoniveau gemäß den zuvor festgelegten Kennzahlen akzeptabel ist. Schließlich werden, wo dies für notwendig erachtet wird, Risikominderungsmaßnahmen und Maßnahmen zur Verbesserung der Systemsicherheit auf der Grundlage von Prioritäten, des Unternehmensbudgets und der Notwendigkeit der Einhaltung geltender Vorschriften festgelegt. Alle Entscheidungen

werden unter Berücksichtigung des Wertes der zu schützenden Informationen und des Eintretens von Ereignissen getroffen, die die Systemsicherheit erheblich beeinträchtigen könnten.

VERANTWORTLICHKEITEN

Die Verantwortlichkeiten sind wie folgt verteilt:

DAS PERSONAL, das für die Einhaltung der vereinbarten Informationssicherheitsrichtlinie verantwortlich ist und jegliche festgestellten Auffälligkeiten dem zuständigen Verantwortlichen melden muss.

DAS INFORMATIONSSICHERHEITSKOMITEE, das mindestens alle sechs Monate zusammentritt. Es besteht aus der Geschäftsleitung und dem Informationssicherheitsbeauftragten, wobei bei der Bewertung spezifischer Fragestellungen auch Mitarbeiter mit dem erforderlichen technischen Fachwissen einbezogen werden können. Die Geschäftsleitung ist verantwortlich für die Festlegung von Prioritäten und die Förderung von Initiativen im Bereich der Informationssicherheit, wobei sie die Abstimmung mit den Unternehmensstrategien und dem für das Projekt vorgesehenen Budget sicherstellt.

DER INFORMATIONSSICHERHEITSBEAUFTRAGTE, der für die Ausarbeitung und Gestaltung des Informationssicherheits-Managementsystems verantwortlich ist. Insbesondere führt der Informationssicherheitsbeauftragte die Risikoanalyse und das Risikomanagement durch, indem er die geeignetsten Kriterien und Methoden identifiziert, und ist für die Führung der notwendigen Dokumentation, einschließlich der Verfahren zur Klassifizierung von Dokumenten, verantwortlich. Die Rolle umfasst zudem den Vorschlag geeigneter Sicherheitsmaßnahmen und die Überprüfung von Sicherheitsvorfällen samt der zugehörigen Korrekturmaßnahmen. Darüber hinaus setzt sich der Informationssicherheitsbeauftragte dafür ein, eine Kultur der Informationssicherheit zu fördern und Schulungsprogramme für das Personal vorzuschlagen.

EXTERNE PARTEIEN, die mit Artificialy SA interagieren, müssen die festgelegten Sicherheitsgrundsätze einhalten und, sofern dies nicht ausdrücklich im Vertrag vorgesehen ist, eine Vertraulichkeitsvereinbarung für den ihnen zugewiesenen Auftrag unterzeichnen.

ANWENDBARKEIT

Diese Informationssicherheitsrichtlinie gilt für alle internen und externen Stellen des Unternehmens und ist für das gesamte Personal von Artificialy SA verbindlich. Sie gilt zudem für jede externe Partei, die Kenntnis von durch das Unternehmen verwalteten Informationen erlangt. Dies erfordert eine vorherige Regelung von Vereinbarungen, um

sicherzustellen, dass die Kommunikation mit externen Parteien im Einklang mit den geltenden Regeln und Vorschriften erfolgt.

ÜBERPRÜFUNG

Artificialy SA gewährleistet die regelmäßige Überprüfung der Wirksamkeit und Effizienz des Informationssicherheits-Managementsystems. Wo erforderlich und im Einklang mit dem Kontext und den Unternehmenszielen, ergreift es die notwendigen Maßnahmen zur Verbesserung der Sicherheitsrichtlinien und zur Gewährleistung ihrer ordnungsgemäßen Umsetzung, um die kontinuierliche und sichere Durchführung aller Unternehmensprozesse zu gewährleisten.