Leitlinie Informationssicherheit

Dokumententyp	Richtlinie
Version	2.1
Datum	07.08.2024
Eigentümer	Geschäftsführung (Tobias Tiedgen)
Klassifikation	öffentlich
Verteilerkreis	d.vinci

Unternehmen & Geschäftszweck

Unser Unternehmen ist Auftragsverarbeiter und Anbieter von Lösungen rund um das Themenfeld "Mitarbeitergewinnung".

Unsere Standardsoftware-Lösungen werden von Personalabteilungen anderer Unternehmen eingesetzt, um die Daten von Bewerber:innen und angehenden Mitarbeiter:innen zu verwalten. Weiterhin bieten wir unseren Kund:innen Beratung und Dienstleistungen rund um das Thema Recruiting an.
Die Softwareentwicklung, der Betrieb, der Vertrieb, die Beratung, die Dienstleistungen sowie der Service/Support erfolgen in unserem Hause am Standort Hamburg.

Unsere Kund:innen vertrauen uns im Rahmen der Software-Nutzung als auch bei Projekten zahlreiche sensible Daten an (bspw. Bewerberdaten, aber auch Betriebsgeheimnisse). Diese zu schützen, ist für unser Unternehmen existenziell notwendig - ein Datenverlust kann Schäden zur Folge haben, die für unser Unternehmen (lebens-)bedrohlich wären.
Daher ist es eines unserer wesentlichen Ziele, sensible und personenbezogene Daten vertraulich zu behandeln und in hohem Maße zu schützen. Weiterhin ist es unser Ziel, die IT-Systeme in ihrer Verfügbarkeit so zu sichern, dass Ausfallzeiten auf ein tolerierbares Minimum begrenzt werden und ein Datenverlust soweit wie möglich ausgeschlossen wird.

Auch in der Zusammenarbeit mit Dienstleistern, Lieferanten und Partnern stellen wir sicher, dass die Informationssicherheit jederzeit gewährleistet ist, um unsere Werte zu schützen und unsere Sicherheitsziele zu erreichen.

Die Zertifizierung nach ISO/IEC 27001 stellt für uns einen großen Wettbewerbsvorteil gegenüber unseren Marktbegleitern dar. Wir zeigen unseren Kund:innen hiermit transparent und unmissverständlich, dass wir die uns anvertrauten Daten professionell schützen und wir uns ihren Anforderungen an Informationssicherheit verpflichtet fühlen.

Scope dieser Leitlinie

Der Markt erwartet von unserem Unternehmen nicht nur qualitativ hochwertige Beratung, Software und Dienstleistungen, sondern auch die Sicherstellung der Informationssicherheit. Dies können wir nur gemeinsam als Team gewährleisten, da wir alle zu jeder Zeit unseren Beitrag zur Informationssicherheit leisten.
Somit gilt diese Leitlinie für alle unsere Unternehmensbereiche und alle unsere Prozesse.

Ziele & Anforderungen

Unser höchstes Gut ist das Vertrauen unserer Kund:innen!
Dieses Vertrauen und damit letztlich der Erfolg unseres Unternehmens beruhen darauf, dass wir insbesondere

- eine hohe Professionalität und Qualität unserer Beratung, Software und Dienstleistungen sicherstellen
- unsere Softwarelösungen innovativ, aber gleichzeitig robust und sicher gestalten
- Ausfälle auf ein tolerierbares Minimum begrenzen
- Datenverlust, soweit technisch und betriebswirtschaftlich möglich, ausschließen
- die Integrität und Vertraulichkeit von personenbezogenen und schützenswerten Daten wahren
- Betriebsgeheimnisse schützen
- Datenschutzgesetze und gesetzliche Rahmenbedingungen einhalten

Es ist daher für uns existenziell notwendig, diese Anforderungen bei unserem täglichen Tun zu berücksichtigen und uns mit den bestehenden Risiken auseinanderzusetzen.

Auch wenn sich Sicherheitsvorfälle nie ganz vermeiden lassen: Es ist unser Ziel, Risiken im Vorwege zu erkennen, dass wir Sicherheitsvorfälle zügig erkennen, geeignete Gegenmaßnahmen einleiten können, daraus lernen und kein Schaden für unsere Kunden und Mitarbeiter entsteht.
Daher betrachten wir in allen Projekten, Prozessen und Entscheidungen die Anforderungen an die Informationssicherheit sowie potenzielle Risiken und Chancen.

Unser Miteinander basiert auf Vertrauen! Nach innen (intern) sorgen wir für größtmögliche Transparenz und Offenheit; jede:r Mitarbeiter:in soll auf alle Informationen zugreifen können, damit jede:r Erfahrungen, Learnings und Wissen schnellstmöglich zur Verfügung haben (außer in begründeten Ausnahmen).

Nach außen (extern) sorgen wir für höchstmögliche Vertraulichkeit; wir kommunizieren schützenswerte Informationen nur explizit dem Empfänger auf einem jeweils angemessen sicheren Kommunikationsweg.

Mitwirkung & Integration im Unternehmen

Alle Teammitglieder tragen ihren Teil zur Informationssicherheit bei, indem sie

- sich bewusst sind, welche Risiken wir als Unternehmen tragen, wenn die Informationssicherheit bewusst oder unbewusst verletzt wird
- verstehen, wann ein Problem einen Informationssicherheitsvorfall darstellt und diesen melden
- die oben genannten Grundsätze befolgen
- Werte und wahrgenommene Risiken benennen
- an der ständigen Verbesserung der Informationssicherheit sowie des ISMS mitwirken (Audits, Feedback, etc.)

Jede:r von uns erhält regelmäßig Schulungen und Wissensvermittlung zum Thema Informationssicherheit. Sofern spezielle Sicherheitsregeln für einen Arbeitsplatz erforderlich sind, erhalten die betreffenden Personen hierzu eine separate An- und Einweisung. Wir erwarten von allen Teammitgliedern, dass sie diese Punkte sowie die relevanten Vereinbarungen & Regeln kennen und diese in ihrer täglichen Arbeit anwenden.

d.vinci hat einen internen Informationssicherheitsbeauftragten, der das ISMS aufrechterhält und weiterentwickelt. Hierzu ist er auch verantwortlich dafür, Sachverhalte anzusprechen, bei denen ggf. Auswirkungen auf die Informationssicherheit zu erwarten sind. Unser Informationssicherheitsbeauftragter ist auch erster Ansprechpartner für alle Vorfälle der IT-Sicherheit und hält Kontakt zu Behörden sowie Interessensgruppen.

Das Informationssicherheitsmanagementsystem (ISMS)

Das Informationssicherheitsmanagementsystem (ISMS) soll kein Schattendasein führen, sondern in der tagtäglichen Arbeit aller Teammitglieder verankert sein, ohne als "Ballast" wahrgenommen zu werden.

Dazu wünschen wir uns eine pragmatische Umsetzung der ISO-Norm, dies bedeutet insbesondere:

- so wenig wie möglich, so viel wie nötig (oder auch: Weniger ist mehr!)
- Dokumente, die leicht verständlich sind und gerne gelesen werden
- praktikable Methode zur Risikobewertung, die sich an unserem Bedarf orientiert
- das System lernfähig zu halten, indem wir es regelmäßig überprüfen und verbessern

Wir glauben, dass das Wissen unserer Mitarbeitenden die beste Basis für stetige Verbesserung ist. Wir ergreifen Maßnahmen, um das Feedback und das Wissen der Mitarbeiter:innen transparent zu machen und in die Verbesserung des ISMS mit einfließen zu lassen. Ebenso wünschen wir uns jederzeitiges Feedback von Mitarbeiter:innen über die Wahrnehmung und Wirksamkeit des ISMS.

Weiterhin lassen wir das System regelmäßig extern und intern auditieren, um Verbesserungspotenziale zu erkennen und umzusetzen.

Wichtige Dokumente

Diese Dokumente solltest du als Teammitglied unbedingt kennen:

Leitlinie Datenschutz (die andere Seite derselben Medaille)
Rollen und Vertreter
Sicherheitsrichtlinie IT-Nutzung