ISO 27001: 2013 Konformität

Selbsterklärung

Innerhalb der Diehl-Gruppe wird ein hohes Niveau der Informationssicherheit und des Datenschutzes aufrechterhalten. Um dieses Niveau zu erreichen, betreiben wir ein konzernweites Informationssicherheits-Managementsystem (ISMS)[1] , das sich im Wesentlichen an der ISO 27001 orientiert.
Das eingeführte, prozessorientierte Integrierte Managementsystem bildet den Rahmen für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; durch die Anwendung eines Risikomanagementprozesses gibt es den interessierten Parteien die Gewissheit, dass die Risiken angemessen gesteuert werden.
Das ISMS[2] basiert auf den für die gesamte Diehl-Gruppe gültigen Regelungen, wie Richtlinien und Leitfäden, und wird regelmäßig durch interne Sicherheitsaudits überprüft. Darüber hinaus umfassen diese Audits auch technische Prüfungen, wie z.B. Penetration Tests unserer internen IT-Infrastruktur.
Auf Basis dieser interner Vorschriften, die unseren Mindeststandard für das Informationssicherheitsmanagement darstellen, konnte jede Unternehmenseinheit die Einhaltung der Anforderungen der ISO 27001 nachweisen.
Die Hauptelemente unseres ISMS entsprechen dem Diehl-Leitfaden "20 goldene Regeln", der wiederum den Anforderungen der ISO 27001 entspricht:

- Verantwortung des Managements
- Risikomanagement
- Angemessener Umgang mit Informationen
- Erstellung von IS-Regelungen
- Sensibilisierung der Mitarbeiter
- Eindeutige Festlegung von Zuständigkeiten und Kompetenzen
- Genehmigung und Kontrolle von neuen IT-Ressourcen und IT-Verfahren
- Verschlüsselte Übermittlung sensitiver Informationen über öffentliche Netze
- Keine Internetanbindung ohne Firewall
- Angemessene Überwachung von Zugriffen
- Regelmäßige Datensicherung
- Beachtung von geltendem Recht
- Absicherung von Risiken, die von Externen ausgehen
- Physikalische Absicherung sensitiver Bereiche
- Störungsfreier IT-Betrieb
- Umgang mit Sicherheitsvorfällen - Notfallplanung
- Sicherheit in der Softwareentwicklung
- Änderungsmanagement in Finanz-/ Personal- und Warenwirtschaftssystemen (ERP-Systemen)
- Benutzerverwaltung in sicherheitsrelevanten Systemen
- Sicherer Umgang mit und Entsorgung von Datenträgern

IZAR PLUS Portal ist eine webbasierte Anwendung der Zählerdatenmanagement-Software von Diehl Metering, die als Service in einem nach ISO 27001 zertifizierten Hochsicherheitsrechenzentrum in Deutschland läuft. Der Geltungsbereich der Zertifizierung ist "Conception, transformation, transition and service delivery for managed infrastructure and managed digital workplace ".
Die wichtigsten IT-/Kernsysteme und Daten von Diehl Metering werden von der Diehl Informatik betreut, die ebenfalls zur Diehl-Gruppe gehört. Die Diehl Informatik GmbH ist nach ISO 27001[1] zertifiziert – Geltungsbereich: "Consulting, development, operation and maintenance of information and communication systems".

Dr C. Bosbach A. Geuther R. Edel

Nuremberg, September 06, 2021

[1] ISO 27001 : 2013 Informationstechnik - Sicherheitstechniken - Managementsysteme für Informationssicherheit – Anforderungen
[2] ISMS - Information Security Management System