Gesch.-Nr.: 0009-2023-O30

Informationssicherheitspolitik
im Unternehmen ČD Cargo, a.s.

Das Unternehmen **ČD Cargo, a. s.,** mit Sitz in Praha, Jankovcova 1569/2c, PLZ 170 00, HR-Nr.: 28196678, ist kraft Entscheidung des Nationalen Amtes für Cyber- und Informationssicherheit, gemäß § 22a, Abs.1 von Gesetz Nr. 181/2014 Slg., über Cyber-Sicherheit vom 6.12.2021 **Betreiber folgender Grunddienstleistung: Betrieb von Schienenverkehr oder Dienstleistungseinrichtungen.** Das Informationssystem, von dem diese Dienstleistung abhängig ist, ist das Informationssystem einer Grunddienstleistung.
ČD Cargo hat das Information Security Management System (ISMS bzw. Managementsystem für Informationssicherheit) gemäß der Norm ČSN EN ISO/IEC 27001 eingeführt.

Ziele der Informationssicherheitspolitik

Die Informationssicherheitspolitik definiert die Grundregeln zur Gewährleistung des Schutzes der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen bei der internen und externen Kommunikation. Das Unternehmen ČD Cargo, a.s. verpflichtet sich zum Schutz der Informationen und zur Gewährleistung der Cyber- und Informationssicherheit und deklariert hierdurch gleichzeitig seine Verpflichtungen zum Erreichen seiner definierten Sicherheitsziele, die da sind:

- alle, die Cyber-Sicherheit betreffender Rechtsvorschriften, namentlich gemäß Gesetz Nr. 181/2014 Slg., Ges. über Cyber-Sicherheit **einzuhalten**;
- den Schutz personengebundener Informationen laut der DSGVO-Verordnung und Gesetz Nr. 110/2019 Slg., über die Verarbeitung personenbezogener **sicherzustellen**;
- das Risiko eines möglichen Informationsverlustes oder -missbrauchs **zu minimieren**;
- die Folgen eventueller Cybersicherheitsvorfälle **zu verringern**;
- die ökonomische Tragbarkeit der verwirklichten Maßnahmen für den Daten- und Informationsschutz zur Aufrechterhaltung einer nachhaltigen Entwicklung **zu berücksichtigen**;
- für die effektive Auswahl von Sicherheitsmaßnahmen für den Daten- und Informationsschutz auf der Basis einer kontinuierlich durchgeführten Risikobewertung **zu sorgen**;

- Kompetenzen für die einzelnen Gebiete der Informationssicherheit unter Verwendung eines Systems von Sicherheitsfunktionen und -rollen **zuzuteilen;**
- durch Anwendung eines komplexen Systems der Sicherheitsfortbildung für die Kenntnis der Sicherheitsverfahren bei den Mitarbeitern **zu sorgen**;
- in Form regelmäßiger spezieller Schulungen auf dem Gebiet der Cyber- und Informationssicherheit für die entsprechende Qualifikation der mit der Ausübung von Sicherheitsrollen beauftragten Mitarbeiter **zu sorgen**;
- die Zusammenarbeit mit staatlichen Behörden und Berufsorganisationen **zu vertiefen**, welche die Standards und bestimmenden Grundsätze auf dem Gebiet des Daten- und Informationsschutzes erstellen;
- relevante Sicherheitskriterien bei der Auswahl von Dienstleistungserbringern und Produktlieferanten beim Abschluss von Geschäftsbeziehungen **anzuwenden,** um ein Höchstmaß an Sicherheit bei erbrachten Dienstleistungen zu gewährleisten;
- **systematisch** die Einflüsse aller Tätigkeiten des Unternehmens zum Schutz der Daten- und Informationssicherheit **auszuwerte**n, um deren anhaltenden Schutz zu gewährleisten.

Umfang und Grenzen von Sicherheitsinformationen

Diese Informationssicherheitspolitik bezieht sich auf das gesamte Unternehmen ČD Cargo, a.s., all seine Mitarbeiter und sämtliche Informationen, die auf irgendeine Weise verarbeitet, übermittelt oder gespeichert werden. Die Informationssicherheitspolitik spezifiziert die Sicherheitsregeln und -grundsätze, zu deren Einhaltung sowohl die Mitarbeiter der ČD Cargo, a.s. bei ihren Tätigkeiten, als auch externe Subjekte, die sich auf der Basis einer Geschäftsbeziehung an der Ausübung der Rollen im Informationssystem von ČD Cargo, a.s. beteiligen, oder ggf. externe Subjekte, die an der Verarbeitung, Übermittlung oder Speicherung von Informationen der ČD Cargo, a.s., beteiligt sind, verpflichtet sind. Der Umfang des Systems des Informationssicherheitsmanagements ist per interner Norm der ČD Cargo, a.s. festgelegt.

Grundsätze und Prinzipien der Informationssicherheit

- **Festlegung** von Regeln, Kompetenzen und Folgen im Falle der Verstößen gegen die Sicherheitsgrundsätze;
- **Einhaltung** aller legislativen und vertraglichen Anforderungen für das Gebiet der Informationssicherheit;
- **Fortbildung** aller Mitarbeiter und Subjekte, die für interne Outsourcing-Prozesse auf dem Gebiet der Informationssicherheit sorgen, als risikovollstes Zwischenglied bei der Gewährleistung der Informationssicherheit;
- **Gewährleistung** der Kontinuität von Tätigkeiten zur Lösung von Krisensituationen;

- **Annahme** technischer Präventiv- und Abhilfemaßnahmen im Informationssystem der ČD Cargo, a.s.

Cybersicherheitsvorfälle

Mit Sicherheitsinformationen verbundene Cybersicherheitsvorfälle werden in der ČD Cargo, a.s., kontinuierlich identifiziert und gemanagt. Zur Bewältigung von Cyber- Informationssicherheitsvorfällen werden Maßnahmen getroffen; entsprechende Trends von Vorfällen werden mit dem Ziel ausgewertet, die Möglichkeiten zu verbessern, ihnen zuvorzukommen.

Risikomanagement

Das Unternehmen ČD Cargo, a.s., hat in Einklang mit den Empfehlungen der Norm ČSN ISO/IEC 27005 ein Informationsrisikomanagement eingeführt. Informationssicherheitsrisiken werden systematisch ausgewertet und es werden entsprechende Maßnahmen zu deren Reduzierung auf ein akzeptierbares Risikomaß getroffen.

Erklärung der Unternehmensleitung von ČD Cargo, a.s.

Die Unternehmensleitung der ČD Cargo, a.s., verpflichtet sich getreu dieser Politik zum Informationsschutz und zur Gewährleistung der Cyber- und Informationssicherheit. Gleichzeitig deklariert sie hiermit ihre Verpflichtungen zum Erreichen der definierten Ziele für die Cyber- und Informationssicherheit.

Cargo Ing. Tomáš Tóth 2023.02.21 13:58:28 +01'00'

Ing. Tomáš Tóth
Vorstandsvorsitzender

Ing. Marek Hejduk, MPA Digitálně podepsal Ing. Marek Hejduk, MPA Datum: 2023.02.03 08:09:01 +01'00'

Ing. Marek Hejduk, MPA
Sicherheitsdirektor