

Informationssicherheitspolitik

der

dedica Genossenschaft

1 Grundsatz und Geltungsbereich

Informationssicherheit ist ein Bestandteil unserer Geschäftsstrategie und der Geschäftsziele. Um deren Nachweis zu erbringen, orientiert sich dedica an ISO/IEC 27001. Die Informationssicherheit umfasst alle Bereiche der dedica Genossenschaft.

2 Verpflichtung

Informationssicherheit ist Sache des gesamten Unternehmens und aller Beteiligten: Bei unseren Mitarbeitenden wird auf allen Ebenen das Verantwortungsbewusstsein für die Informationssicherheit geschult und gefördert. Wir verpflichten uns zum Einsatz einer zeitgemässen und verfügbaren Technologie unter Berücksichtigung der wirtschaftlichen Möglichkeiten. Die Einhaltung aller gesetzlichen, behördlichen oder kundenspezifischen Anforderungen ist selbstverständlich. Darüber hinaus verpflichten wir uns, die Informationssicherheit kontinuierlich zu verbessern.

3 Zielsetzung

dedica setzt sich folgende Zielsetzung:

- Wir sichern die Vertraulichkeit, Integrität und Verfügbarkeit der uns anvertrauten Informationen
- Wir setzen uns für eine ständige Verbesserung des ISMS (Informationssicherheitsmanagementsystem) ein und entwickeln dies deshalb laufend weiter
- Wir richten die Ausgestaltung des ISMS nach der ISO 27001 Norm
- Wir verhindern Strafverfolgung und Haftungsansprüche durch Einhaltung gesetzlicher (Gesetzes-Konformität) und vertraglicher Verpflichtungen

4 Umsetzung und kontinuierliche Verbesserung

Wir betreiben ein Informationssicherheits-Managementsystem (ISMS) mit dem Ziel, die Informationssicherheit gezielt zu fördern und die Leistung der Unternehmung kontinuierlich zu verbessern. Das ISMS bildet einen integrierten Bestandteil unseres Managementsystems. Im Besonderen das Risikomanagement ist in Bezug auf die Informationssicherheit umfassend umgesetzt. Prozesse und Abläufe sind so definiert, dass die Informationssicherheit eingehalten wird. In regelmässigen Abständen wird das komplette System auditiert, auch Leistungen von Drittparteien. Nichterfüllung und Nichterreicherung einer Zielsetzung wird zum Anlass ge-

nommen, das System zu verbessern und eine nachhaltige Veränderung der Kultur und Arbeitsweise im Betrieb zu erreichen, welche auch künftige kontinuierliche Verbesserung sicherstellt, damit ein nachhaltiger Mehrwert für die Firma entsteht.

5 Organisation und Verpflichtungen

5.1 Geschäftsleitung

Die Geschäftsleitung ist Auftraggeberin der Informationssicherheitsbeauftragten Person (ISB). Die Geschäftsleitung definiert die Strategie und setzt strategische Ziele im Bereich der Informationssicherheitspolitik.

5.2 Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte (ISB bzw. CISO – Chief Information Security Officer gemäss ISO 27001) verantwortet, überwacht und verbessert das ISMS, setzt die definierten Ziele um und rapportiert zu Händen der Geschäftsleitung.

5.3 Mitarbeitende

Mitarbeitende auf allen Stufen sind verantwortlich für die Einhaltung der Informationssicherheit. Unterstützt und geschult werden sie durch die Linienvorgesetzten und die Querschnittsfunktion Informationssicherheit.

5.4 Externe Mitarbeiter

Externe Mitarbeitende sind verpflichtet, die Informationssicherheit innerhalb des Geltungsbereiches, in welchem sie eine Leistung erbringen, einzuhalten. Unterstützt und geschult werden sie durch den internen Auftraggeber.

5.5 Lieferanten und Drittparteien

Bei der Zusammenarbeit mit Dritten und bei der Auswahl der Lieferanten ist Informationssicherheit ein wichtiges Kriterium, diese müssen die Vorgaben der dedica anwenden. Dazu werden vertragliche Regelungen getroffen. Dedicca behält sich das Recht vor, deren Regeln jederzeit unangekündigt zu auditieren.

5.6 Sanktionen

Verstösse gegen die Vorgaben betreffend Informationssicherheit werden nicht geduldet und werden geahndet. Mit Drittparteien werden Konventionalstrafen vereinbart, bei Mitarbeitern kommen arbeitsrechtliche Sanktionen zur Anwendung.

Thun, 21.11.2019
Der Verwaltungsrat