Informationssicherheitspolitik Spezialleistungen

Die Informationssicherheit hat einen hohen Stellenwert bei Spezialleistungen und ist ein Bestandteil der Geschäftsstrategie und Geschäftsziele. Aus diesem Grund wird ein ISMS nach ISO 27001 unterhalten. Entsprechende Rollen und Kompetenzen sind definiert.

Verantwortlichkeit

Informationssicherheit ist Sache Aller: Bei den Mitarbeitenden wird auf allen Ebenen das Verantwortungsbewusstsein für die Informationssicherheit geschult und gefördert. Die Spezialleistungen verpflichtet sich zum Einsatz der besten verfügbaren Technologie unter Berücksichtigung der wirtschaftlichen Möglichkeiten. Die Einhaltung aller einschlägigen Anforderungen (gesetzlich, behördlich und bezüglich Kundenforderungen) ist selbstverständlich. Darüber hinaus verpflichtet sich die Spezialleistungen, kontinuierlich an der Verbesserung der Informationssicherheit zu arbeiten.

Die Geschäftsleitung unterstützt die Informationssicherheitstätigkeiten mit den notwendigen Ressourcen. Zudem prüft sie die Einhaltung der Regeln und trifft bei Abweichungen entsprechende Massnahmen.

Der Sicherheitsverantwortliche (CISO – Chief Information Security Officer) verantwortet, überwacht und verbessert das ISMS, setzt die definierten Ziele um und rapportiert der Geschäftsleitung.

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

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.

Ziele

Die Spezialleistungen hat im Bereich der Informationssicherheit folgende Ziele definiert:

- Aufbau und Weiterentwicklung einer geeigneten Sicherheitsorganisation,
- Schulen eines sicherheitsgerechten Verhaltens am Arbeitsplatz,
- Sicherheitsschutz vor Angriffen aus dem Internet, wie auch vor Malware und anderen Schädlingen,
- ermöglichen eines sicheren mobilen Arbeitens unterwegs und im Home-Office,
- auf die Rolle eingeschränkte Berechtigungen für Mitarbeitende und Administratoren,
- Reduktion der Schäden durch potenzielle Vorfälle,
- Einhaltung der Datenschutz- und Datensicherheitsrichtlinien und -bestimmungen (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit),
- Einhaltung der Gesetze und vertraglichen Anforderungen.

Informationssicherheits-Managementsystem (ISMS)

Die Spezialleistungen betreibt ein ISMS mit dem Ziel, die Informationssicherheit gezielt zu fördern und die Leistung der Unternehmung kontinuierlich zu verbessern. Das ISMS bildet einen integrierten Bestandteil des QMS. 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 Nichterreichung einer Zielsetzung wird zum Anlass genommen, 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.

Dritte

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

Verstösse

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