Informationssicherheitsmanagement
Leitlinie Informationssicherheit

Inhaltsverzeichnis

1 Leitgedanke und Stellenwert der Informationssicherheit

Die Ideen und das Fachwissen unserer Mitarbeiter sind das Fundament unseres Erfolgs. Die Verfügbarkeit unserer Betriebsstätten, Anlagen und Systeme sowie unsere Erreichbarkeit spiegelt die Verlässlichkeit gegenüber Kunden und Geschäftspartnern wider und trägt maßgeblich zum guten Ruf unseres Unternehmens bei. Um diese Werte zu schützen, schafft unser Unternehmen ein weltweites, angemessenes Schutzniveau für die Vertraulichkeit, Integrität (Korrektheit) und Verfügbarkeit unserer Prozesse, Informationen und Systeme.

Dem erklärten Unternehmensziel, zentrale Geschäftsprozesse mitsamt dort benötigten Informationswerten und IT-Systemen effektiv zu schützen, wird durch die Schaffung global gültiger Sicherheits-standards und die Integration von Informationssicherheit in interne Prozesse entsprochen. Die definierten Informationssicherheitsziele tragen dabei zur Erreichung der Unternehmensziele bei.

Ein stets vorhandenes Bewusstsein im Bereich Informationssicherheit bei allen täglich anfallenden Aktivitäten wird von jedem Mitarbeiter erwartet. Jeder Vorgesetzte ist verpflichtet, die Einhaltung der Vorschriften zur Informationssicherheit durch seine Mitarbeiter sicherzustellen und zu kontrollieren. Jeder Mitarbeiter, der Schwachstellen im Bereich der Informationssicherheit erkennt, ist verpflichtet, diese seinem Vorgesetzten oder dem Informationssicherheitsbeauftragten mitzuteilen.

2 Unser Fachwissen, unser Vorsprung

Sorgfalt und Genauigkeit im Umgang mit Informationen

Need-to-Know Prinzip

Informationen sind nur an die Personen und Stellen weiterzugeben, die diese auch benötigen. Den beteiligten Personen muss dabei klar sein, wie vertraulich Informationen sind und für wen sie bestimmt sind. Das gilt auch für Berechtigungen in IT-Systemen und für Zutrittsrechte.

Richtiger Umgang mit Dokumenten und Datenträgern

Der Umgang mit Dokumenten und Datenträgern mit vertraulichem Inhalt ist ein zentraler Punkt beim Schutz von Informationen. Sparsamkeit beim Ausdrucken von sensiblen Informationen, die sichere Aufbewahrung von Dokumenten und Speichermedien in verschlossenen Bereichen sowie die ordnungsgemäße Entsorgung liegen in der Verantwortung eines jeden Mitarbeiters.

Technische Sicherheit

Das Sicherheitsniveau kann durch technische Mittel maßgeblich gestärkt werden. Zielgerichtete Investitionen in die Absicherung sowie eine sichere Konzeption unserer IT und unserer Gebäude gehören deshalb ebenfalls zur Strategie der Absicherung. Dabei liegt uns besonders am Herzen, unsere wichtigsten und sensibelsten Einrichtungen zu schützen.

Eigenverantwortung

Jeder Mitarbeiter steht in der Verantwortung, Schwachstellen, verdächtige Situationen und Vorfälle zu melden. Das Kennen und Beachten von Vorgaben durch unsere Mitarbeiter werden dabei als Voraussetzung gesehen und von jedem Mitarbeiter erwartet.

Umsetzung

Das Unternehmen setzt zur Sicherstellung der Umsetzung von Informationssicherheitsanforderungen ein Informationssicherheitsmanagementsystem (ISMS) in Anlehnung an den internationalen Standard ISO/IEC 27001 ein. Des Weiteren werden gesetzliche und vertragliche Anforderungen berücksichtigt.

Das ISMS folgt dem dort empfohlenen kontinuierlichen Verbesserungsprozess auf Basis des PDCA-Modells (Plan, Do, Check, Act). Ziel ist es, nachweislich und regelmäßig die Angemessenheit, Vollständigkeit, Nachhaltigkeit, Effektivität und Effizienz der implementierten Informationssicherheitsprozesse und Schutzmaßnahmen sicherzustellen.

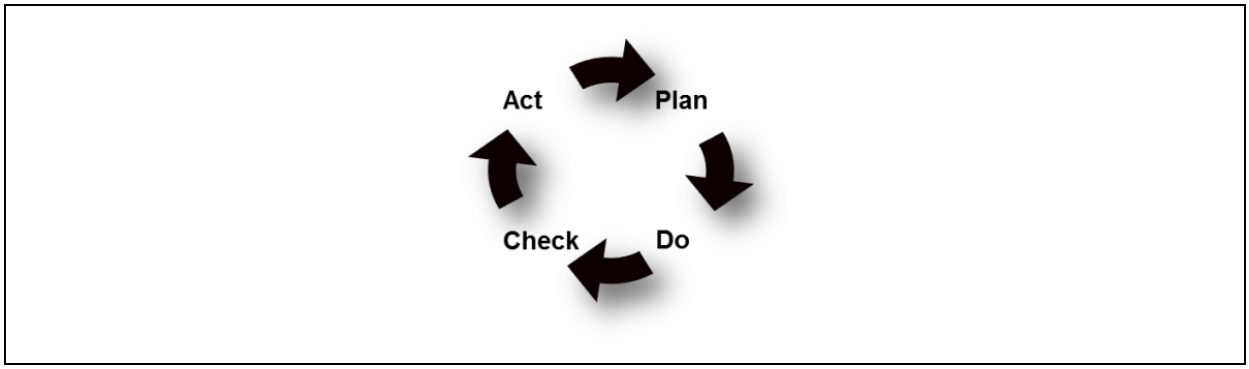

Abbildung 1: PDCA-Modell

PLAN - Festlegen des ISMS: Die Strategien, Ziele, Prozesse, Regelungen, Verfahren, Methoden, Werkzeuge und Verantwortlichkeiten des ISMS werden festgelegt.

DO - Umsetzen und Durchführen des ISMS: Die definierten Prozesse, Regelungen und Verfahren werden entsprechend der Ziele des ISMS umgesetzt. Ausgewählte Maßnahmen werden implementiert.

CHECK - Überwachen und Überprüfen des ISMS: Anhand praktischer Erfahrungen, den Ergebnissen von Audits und Managementbewertungen werden die Prozesse, Wirksamkeit und Effizienz der gewählten Ansätze und Maßnahmen gemessen und überprüft. Es wird identifiziert, ob Handlungsbedarf besteht und an welchen Stellen Optimierungsmöglichkeiten vorhanden sind.

ACT - Instandhalten und Verbessern des ISMS: Basierend auf den Ergebnissen der Phase Check und sonstiger Rückmeldungen (z.B. aktuelle Risikosituation / Bedrohungslage / Weiterentwicklungen / Anforderungen), werden Korrektur- und Vorbeugemaßnahmen ergriffen, die zu einer fortlaufenden Verbesserung des ISMS und des Sicherheitsniveaus führen. Die Behandlung von Sicherheitsvorfällen ist eine weitere Aufgabe dieser Phase.

3 Übersicht Prozesse und Richtlinien

4 Verantwortung des Managements

Die Unternehmensleitung ist innerhalb des Unternehmens für die Informationssicherheit verantwortlich und verpflichtet sich dazu, die erforderlichen personellen, organisatorischen und finanziellen Ressourcen bereitzustellen, um ein angemessenes Informationssicherheitsniveau zu etablieren, aufrechtzuerhalten und weiterzuentwickeln.

Im Rahmen ihrer Managementaufgaben und Vorbildfunktion sind alle Führungskräfte in besonderem Maß für die Förderung des vorhandenen Sicherheitsbewusstseins ihrer Mitarbeiter hinsichtlich der Informationssicherheit und IT-Sicherheit verantwortlich.

5 Schlussbestimmungen und Geltungsbereich

Diese Leitlinie wird durch weitere Richtlinien ergänzt, die aus detaillierten Organisations- und Sicherheitsregeln in ausgewählten Bereichen und Länder- sowie standortspezifischen gesetzlichen und organisatorischen Regelungen bestehen. Sie haben, soweit nicht anders gekennzeichnet, den gleichen Geltungsbereich wie diese Leitlinie und sind jeweils ab dem Zeitpunkt ihrer Veröffentlichung gültig. Der Geltungsbereich des zugrunde liegenden Informationssicherheitsmanagementsystems ist zentral festgelegt und im mitgeltenden ISMS Scope Dokument dargestellt und ausgearbeitet.