

Leitlinie zur

Informationssicherheit

1 Kontext

1.1 Einleitung

Die RECPLAST GmbH hat ein Managementsystem für Informationssicherheit (ISMS) etabliert, das dem Regelwerk „IT-Grundschutz“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügt. Zentraler Bestandteil eines ISMS ist ua die Leitlinie zur Informationssicherheit. Das vorliegende Dokument ist die Leitlinie zur Informationssicherheit der RECPLAST GmbH.

1.2 Geltungsbereich

Der Geltungsbereich dieser Leitlinie ist der Geltungsbereich des ISMS, wie in der Strukturanalyse beschrieben. Die Richtlinie gilt für alle Mitarbeiter im Geltungsbereich.

1.3 Ansprechpartner

Ihr Ansprechpartner zu allen Fragen dieser Richtlinie:
Informationssicherheitsbeauftragter (ISB).

1.4 Verantwortlichkeiten

Diese Leitlinie hat die Geschäftsführung der RECPLAST GmbH freigegeben.

2 Stellenwert der Informationstechnologie und Informationssicherheit

Informationssicherheit stellt für die RECPLAST GmbH ein äußerst wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da alle wesentlichen strategischen und operativen Geschäftsprozesse im Unternehmen durch Informationstechnologie (IT) maßgeblich unterstützt werden. Ziel des Unternehmens ist es, die Daten und IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen in ihrer Verfügbarkeit so zu sichern, dass die zu erwartenden Stillstandzeiten und der maximale Datenverlust toleriert werden können. Auch gilt es, die Integrität und Vertraulichkeit von sensiblen Unternehmensdaten und personenbezogenen Daten in ausreichender Weise zu garantieren; hierzu gehören Personaldaten ebenso wie technische Unterlagen. Schadensfälle mit hohen finanziellen Auswirkungen und immaterielle Folgen in Form von Imageschäden für das Unternehmen müssen verhindert werden.

Beeinträchtigungen hinsichtlich der Verfügbarkeit der unternehmenseigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen. Die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, Anwendungen und IT-Systeme werden nicht nur durch Externe bedroht, sondern können auch durch interne Schwachstellen gefährdet werden. Ferner werden

der Informationssicherheit im Hinblick auf Ausschreibungen Vorteile im Markt eingeräumt.

3 Unternehmensziele

Die Geschäftsführung der RECPLAST GmbH hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit. Dies bedeutet im Einzelnen:

Bewusstsein für Informationssicherheit:

Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit können hierbei unterstützen.

Einhaltung von Gesetzen oder Vorschriften:

Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für das Unternehmen relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden. Als wichtigste zu beachtende Rahmenbedingungen gelten dabei:

- o §§ 238-239, 257-261 Handelsgesetzbuch (HGB)
- o § 91 Abs 2 Aktiengesetz (AktG) ODER GmbHG §43 Abs 1 GmbH-Gesetz (GmbHG)
- o Datenschutz-Grundverordnung (DSGVO)
- o Bundesdatenschutzgesetz (BDSG)
- o Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- o Betriebsverfassungsgesetz (BVerfG)
- o ergänzende Kundenanforderungen.

Informationssicherheit unterstützt damit auch die Einhaltung von Gesetzen und Vorschriften.

Funktionale Aufgabenerledigung:

Die Informationstechnik muss so betrieben werden, dass Geschäftsinformationen hinreichend schnell verfügbar sind. Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag bei der Abwicklung von Aufträgen oder anderen wichtigen Geschäftsvorhaben führen, sind nicht tolerierbar. Informationssicherheit unterstützt damit auch eine funktionale Aufgabenerledigung.

Vermeidung materieller Schäden: Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall einer IT-Anwendung oder eines Systems entstehen. Informationssicherheit wirkt damit auch materiellen Schäden entgegen. Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen:

Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen. Auch im Umgang mit elektronischen Dokumenten und Informationen ist daher Geheimhaltungsanweisungen strikt Folge zu leisten.

Vermeidung von Ansehensverlust bzw Imageschaden:

Finanzielle Schäden und ein negatives Image für das Unternehmen müssen verhindert werden. Informationssicherheit vermeidet damit Ansehensverlust und Imageschaden des Unternehmens.

Kontinuierliche Verbesserung:

Und ferner strebt die RECPLAST GmbH die kontinuierliche Verbesserung seiner Prozesse rund um die Informationssicherheit an.

4 Organisation des Managementsystems für Informationssicherheit

Grundsätzlich sind folgende Verantwortlichkeiten innerhalb des ISMS definiert:

4.1 Geschäftsführung (GF)

Die Geschäftsführung ist das oberste Entscheidungsgremium. Sie verabschiedet auf Vorschlag der Informationssicherheitsbeauftragten diese Informationssicherheitsleitlinie. Die Geschäftsführung ist dafür verantwortlich, sicherzustellen, dass das ISMS entsprechend dieser Richtlinie umgesetzt und aktualisiert wird und dass die notwendigen Ressourcen verfügbar sind. Der IT-Leitung und dem Informationssicherheitsbeauftragten werden von der Geschäftsführung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die vom Management festgelegten Sicherheitsziele zu erreichen. Die Geschäftsleitung muss das ISMS mindestens einmal jährlich überprüfen (bzw immer im Falle von erheblichen Änderungen) und freigeben. Zweck dieser Überprüfung durch das Management ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS. Die Gesamtverantwortung für die

ordnungsgemäße und sichere Aufgabenerfüllung (und damit die Informationssicherheit) verbleibt bei der Unternehmensleitung.

4.2 IT-Leitung

Die zentrale Instanz für die operative IT-Sicherheit ist die IT-Leitung. Sie ist für den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich. In Zusammenarbeit mit dem Informationssicherheitsbeauftragten bringt sie die für die Informationssicherheit spezifischen Aspekte und Anliegen ein und ist für die Umsetzung geeigneter Sicherheitsmaßnahmen zuständig. Die IT-Leitung stellt sicher, dass der Informationssicherheitsbeauftragte frühzeitig in alle IT-Projekte eingebunden wird.

4.3 Informationssicherheitsbeauftragter (ISB)

Der Informationssicherheitsbeauftragte ist für die Koordination des Betriebs des ISMS verantwortlich sowie für die Berichterstattung über dessen Leistungsfähigkeit. Er ist des Weiteren für die Koordination bzw. Umsetzung von Informationssicherheitstrainings und -programmen zur Bewusstseinsbildung (Awareness) für Mitarbeitende verantwortlich. Der Informationssicherheitsbeauftragte definiert, welche sich auf Informationssicherheit beziehenden Informationen durch wen und wann kommuniziert werden. Dies gilt sowohl für interne als auch externe Parteien. Er ist für die Aufstellung und Implementierung des Plans für Training und Awareness verantwortlich, dem alle Personen unterliegen, die eine Rolle im ISMS innehaben. Die Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten bedarf einer Freigabe durch den Informationssicherheitsbeauftragten. Dabei muss besonderes Augenmerk darauf gerichtet werden, dass durch den Einsatz der neuen Komponenten und Verfahren die Risiken hinsichtlich Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) nicht erhöht werden. Der Informationssicherheitsbeauftragte berät die Geschäftsführung und die Fachbereiche in Fragen der Informationssicherheit und arbeitet mit der IT-Leitung zusammen. Er beobachtet laufend die technischen und organisatorischen Fortentwicklungen im Bereich der Informationssicherheit und schlägt in Abstimmung mit der IT-Leitung die notwendigen Maßnahmen vor. Des Weiteren ist er frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase alle sicherheitsrelevanten Aspekte berücksichtigen zu können.

4.4 ICS-ISB

ICS-ISB ist die Kurzbezeichnung für den Informationssicherheitsbeauftragten für die Industrial Control Systems. Er arbeitet mit dem Informationssicherheitsbeauftragten zusammen.

4.5 IS-Management-Team (ISMS-Team)

Das IS-Management-Team setzt sich aus dem Informationssicherheitsbeauftragten, dem ICS-ISB sowie fachkundigen Mitarbeitern für die Administration und für den Betrieb zusammen. Das IS-Management- Team hält regelmäßige Treffen ab. Das IS-Management-Team plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung der Informationssicherheit. Weiterhin werden im IS-Management-Team Audits geplant und Sicherheitsvorfälle besprochen. Im IS-Management-Team werden auch die Dokumente des ISMS laufend überprüft und überarbeitet. Planungen und Änderungen im Anwendungsbereich sind stets im IS-Management-Team abzustimmen.

4.6 Mitarbeiter

Die Mitarbeiter sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie sollen verantwortungsbewusst mit den Informationssystemen und den darauf gespeicherten und dort verarbeiteten Daten umgehen und auf die Wahrung von Betriebs- und Geschäftsgeheimnissen achten. Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Werten unterliegt der Verantwortung der Eigentümer der jeweiligen Werte. Bei Unregelmäßigkeiten müssen die Mitarbeiter unverzüglich den Informationssicherheitsbeauftragten und ihre Vorgesetzten informieren. Es wird erwartet, dass jeder Nutzer von IT-Systemen die vorliegende Informationssicherheitsleitlinie kennt und beachtet.

4.7 Weitere Verantwortlichkeiten

Für alle Informationen, Geschäftsprozesse sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (Informations-, Prozess- und Systemeigentümer, Eigentümer von Zielobjekten) benannt. Diese sind dafür zuständig, die geschäftliche Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass die Mitarbeiter dieser Bedeutung entsprechend handeln. Sie verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich und sind gegenüber der Leitung rechenschaftspflichtig. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartnern die Vorgaben der RECPLAST GmbH zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

5 Folgen von Zuwiderhandlungen

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder den Ruf des Unternehmens gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

6 Weitere Maßnahmen

Ausgehend von der IT-Grundsatz-Methodik zur Einführung und Aufrechterhaltung eines Managementsystems für Informationssicherheit wurden diverse weiterführende Regelungen geschaffen, die dieses ISMS konkretisieren und ebenfalls gültig sind.

7 Inkrafttreten

Die Richtlinie tritt zum 01-11-2019 in Kraft. Freigegeben durch: Geschäftsführung Bonn, 26-10-2019, UNTERSCHRIFT GF