ECON

Leitlinie

Informationssicherheit

VERSION 1.0

Inhaltsverzeichnis

1 Vorwort

Als Softwarehersteller sind Informationen die Grundlage unseres Geschäfts. Abstrakt repräsentiert und verarbeitet in Form von Bits und Bytes lässt sich leicht übersehen, worum es sich bei diesen Informationen wirklich handelt: Personenbezogene Daten, Buchhaltungs- und Finanztransaktionen, vertragsrelevante Dokumente oder Unternehmenskennzahlen.

Dass diese Informationen für unsere Geschäftskunden und letztendlich deren Kunden stets sicher verfügbar und für alle anderen unerreichbar sind, ist keine Selbstverständlichkeit und auch kein Ziel, dass ausschließlich durch sicheren Code und geeignete Verschlüsselungsverfahren zu erreichen ist. Informationssicherheit muss für eine Institution gesamtheitlich gedacht und gelebt werden und sollte sich dabei an erprobten und bewährten Praktiken und Standards orientierten.

Aus diesem Grund haben wir in unserem Unternehmen ein Informationssicherheitsmanagementsystem (ISMS) implementiert, das die Aufgabe hat, in einem kontinuierlichen Verbesserungsprozess Informationssicherheit herzustellen, zu erhalten und stetig weiter zu erhöhen.

Hierfür haben wir klare Verantwortlichkeiten für die Informationssicherheit definiert und notwendige Ressourcen und Personal bereitgestellt.

Wir haben ein ISMS-Team zusammengestellt und einen Informationssicherheitsbeauftragten (ISB) ernannt, der alle Tätigkeiten in diesem Bereich initiiert, plant, überwacht und steuert. Der ISB ist zentraler Ansprechpartner für alle Mitarbeiter und Kunden zu Fragen der Informationssicherheit und berichtet direkt an die Geschäftsführung.

Diese Leitlinie zur Informationssicherheit ist dabei maßgebend für den gesamten Informationssicherheitsprozess. Unsere Mitarbeiter sind angehalten, die Vorgaben und Leitlinien zur Informationssicherheit zu beachten und einzuhalten.

Frechen, im September 2021

HP Olbrück
Geschäftsführer

Arne Westphal
Geschäftsführer

Hakan Baran
Geschäftsführer

2 Ziele und Stellenwert der Informationssicherheit

Die Kreativität, das Fachwissen und die Kundenorientierung unserer Mitarbeiter sind das Fundament unseres Erfolgs. Die hohe Verfügbarkeit unserer Systeme und Anwendungen sowie unsere Erreichbarkeit spiegeln die Verlässlichkeit gegenüber Kunden und Geschäftspartnern wider und trägt maßgeblich zum guten Ruf der ECON Application GmbH bei.

Um diese Werte zu schützen schafft unser Unternehmen ein unternehmensweites, angemessenes Schutzniveau für die Vertraulichkeit, Integrität und Verfügbarkeit unserer Prozesse, Informationen und Systeme.

Dem erklärten Unternehmensziel, zentrale Geschäftsprozesse mitsamt den dort verarbeiteten Informationswerten (Primäre Assets) und den dafür erforderlichen IT-Systemen und Prozessen (Unterstützende Assets) effektiv zu schützen, wird durch die Umsetzung national- sowie international anerkannter Sicherheitsnormen in dokumentierte und gelebte interne Prozesse entsprochen. Um diesem Anspruch Nachdruck zu verleihen streben für unser ISMS eine Zertifizierung nach ISO 27001 für das Jahr 2022 an.

Die definierten Informationssicherheitsziele sind zentraler Bestandteil der Unternehmensziele. Ein stets vorhandenes Bewusstsein im Bereich Informationssicherheit bei allen täglich anfallenden Aktivitäten wird von jedem Mitarbeiter erwartet. Jeder Mitarbeiter, der Schwachstellen im Bereich der Informationssicherheit erkennt, ist verpflichtet, diese seinem Vorgesetzten oder dem Informationssicherheitsbeauftragten mitzuteilen.

3 Was wir tun

Least-Privilege-/Need-To-Know-Prinzip

Berechtigungen und Informationen werden restriktiv und nur an die Personen und Stellen vergeben, die diese auch benötigen. Den beteiligten Personen muss dabei klar sein, wie vertraulich Informationen sind und für wen sie bestimmt sind. Das gilt insbesondere für Rollenprofile und Berechtigungen bei 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 sind klar geregelt und 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 der physischen Infrastruktur gehören deshalb ebenfalls zur Strategie der Absicherung. Dabei legen wir besonderen Wert darauf, unsere wichtigsten und sensibelsten Assets zu schützen.

Eigenverantwortung

Informationssicherheit kann nicht durch die isolierte Arbeit einer Stabsstelle erreicht werden, sondern muss in allen Teilen einer Institution gelebt werden. Daher steht jeder Mitarbeiter in der Verantwortung, Schwachstellen, verdächtige Situationen und Vorfälle zu melden. Das Kennen und Beachten von Vorgaben durch unsere Mitarbeiter wird dabei als Voraussetzung gesehen und von jedem Mitarbeiter erwartet. Die dafür notwendige Sensibilisierung der Mitarbeiter erreichen wir durch regelmäßige Schulungen sowohl zur Informationssicherheit als auch speziell zum Datenschutz.

4 Umsetzung

Die ECON Application GmbH setzt zur Sicherstellung der Umsetzung von Informationssicherheitsanforderungen auf ein Informationssicherheitsmanagementsystem (ISMS) in Anlehnung an den internationalen Standard ISO/IEC 27001:2013 sowie an die relevanten gesetzlichen und branchenspezifischen Vorgaben wie dem IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

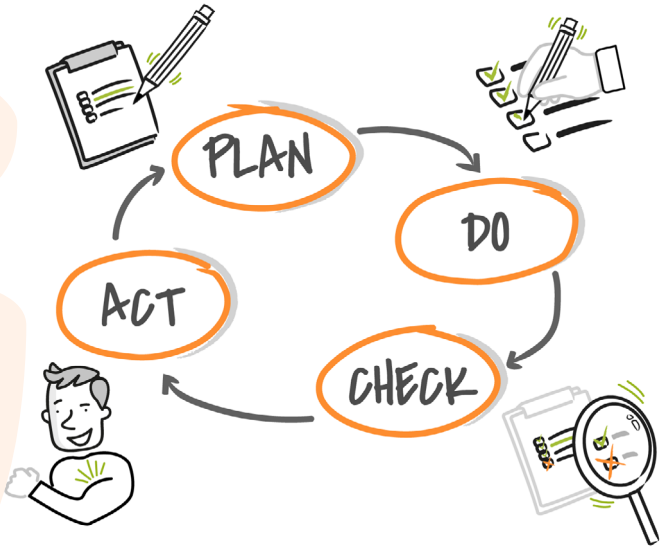
Das ISMS folgt den dort empfohlenen Maßnahmen und dem kontinuierlichen Verbesserungsprozess auf Basis des PDCA-Modells (Plan, Do, Check, Act). Ziel ist es, nachweislich und regelmäßig die Angemessenheit, Vollständigkeit, Nachhaltigkeit, Effektivität und Effizienz der implementierten Informationssicherheitsprozesse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

PLAN – Festlegen

Die Ziele und Verantwortlichkeiten, Prozesse, Regelungen, Verfahren, Methoden und Werkzeuge des ISMS sowie eine Strategie zur Umsetzung werden festgelegt

ACT – Verbessern

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.



DO – Durchführen

Die definierten Prozesse, Regelungen und Verfahren werden entsprechend den Zielen des ISMS umgesetzt. Ausgewählte Maßnahmen werden implementiert.

CHECK – Überprüfen

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.

5 Verantwortung der Geschäftsführung

Die Geschäftsführung 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.

6 Schlussbestimmungen und Geltungsbereich

Diese Leitlinie wird durch eine Reihe weiterer Richtlinien, Prozessbeschreibungen und Arbeitsanweisungen ergänzt, die aus detaillierten Organisations- und Sicherheitsregeln bestehen und daher der internen Verwendung vorbehalten sind.

Der Geltungsbereich (Scope) des Informationssicherheitsmanagementsystems ist genau definiert und wird im mitgeltenden Scope-Dokument beschrieben.

Ansprechpartner

Boris Iven
Informationssicherheitsbeauftragter
Telefon: 02234 91133-47
E-Mail: isb@econ-application.de

ECON Application GmbH
Augustinusstr. 9b
50226 Frechen
www.econ-application.de