	Leitlinie Informationssicherheit	Erstellt von:	Erstellt am:
		Stephan Montag	04.07.2018
		Freigegeben von:	Freigabe am:
		Helga Krueger	01.10.2018
		Klassifikation: öffentlich	Gültigkeitsdauer: drei Jahre

Inhaltsverzeichnis

1. Zweck/Gültigkeitsbereich

Die Organisationsabläufe zur Aufgabenerfüllung in der Herbst Datentechnik GmbH werden durch den Einsatz von Informations- und Kommunikationstechnik (IKT) unterstützt und sind von dieser abhängig. Gleichzeitig erhöhen sich die Risiken und Gefährdungen durch die zunehmende technische Vernetzung und Integration sowie durch die Entwicklung von externen Bedrohungslagen.

Zur Sicherstellung der Erfüllung der Versorgungsaufgaben ist eine Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten weitestgehend zu vermeiden.

Die Geschäftsführung der Herbst Datentechnik GmbH hat mit Datum der Unterzeichnung eine Leitlinie Informationssicherheit beschlossen und in Kraft gesetzt. Als wesentlicher Punkt sieht die Leitlinie die Einführung eines Informationssicherheitsmanagementsystems (ISMS) auf der Grundlage der Norm ISO/IEC 27001:2013 „Informationssicherheits-Managementsysteme". Die sich daraus ergebenden Anforderungen werden in der vorliegenden Leitlinie und ergänzenden Richtlinien, Verfahrensbeschreibungen und Dokumentationen berücksichtigt und umgesetzt. Alle weiteren gesetzlichen Forderungen werden beachtet.

Diese Leitlinie definiert die geforderten Informations-Sicherheitsziele und die damit verbundenen IT-Sicherheitsstrategien, die zum Erfolg des Unternehmens Herbst Datentechnik GmbH entscheidend beitragen.

Die Einhaltung dieser Leitlinie ist verpflichtend für alle Mitarbeiter des Unternehmens sowie für alle externen Mitarbeiter oder Servicekräfte, die mit Daten, Informationen und dem IKT-System des Unternehmens in Berührung kommen.

Die Gewährleistung der Informationssicherheit ist nur sichergestellt, wenn alle Anwender (intern als auch extern) diese definierte Informationssicherheit kennen und dementsprechend verantwortungsvoll anwenden.

Diese Leitlinie dient der Gewährleistung eines sicheren Betriebes der ITK-Infrastruktur der Herbst Datentechnik GmbH im Anwendungsbereich des ISMS und stellt das grundlegende Dokument zur Informationssicherheit dar. In diesem Dokument werden die Ziele, Vorgehensweisen, Organisationsstrukturen sowie Aufgaben für das ISMS festgelegt.

2. Ablauf

2.1 Ziele der Informationssicherheit

Der interne Betrieb und der Informationsaustausch mit anderen Beteiligten wie z.B. Behörden, öffentlichen Einrichtungen, Kunden, Lieferanten, Dienstleistern und Unternehmen können nur auf einer vertrauenswürdigen Basis erfolgen. Voraussetzung dafür sind geeignete technische und organisatorische Maßnahmen, um die Informationssicherheit zu gewährleisten.

Mit dem abgestimmten Vorgehen in der Informationssicherheit soll ein einheitliches Sicherheitsniveau erlangt und datenschutzrechtliche sowie weitere gesetzliche Anforderungen an die Sicherheit der Informationsverarbeitung erfüllt werden.

Durch eine einheitliche Vorgehensweise, die auch mit externen Beteiligten (Dienstleistern) abgestimmt wird, soll eine effiziente und effektive IT-Unterstützung der Betriebsabläufe erfolgen.

Die hohen Investitionen in IT-Systeme müssen zu einer nachhaltigen Verfügbarkeit und Kontinuität des Handelns führen, ohne dass Manipulation, unberechtigter Zugriff und Verlust von Daten zu erwarten ist.

Es soll eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik in den jeweiligen Verantwortungsbereichen erreicht werden. Information, Weiterbildung, Sensibilisierung aller Beschäftigten zu Themen der Informationssicherheit sind hierbei wesentliche Eckpfeiler.

Schutzziele entsprechend der ISO/IEC 27001:2013 sind Vertraulichkeit, Integrität, Verfügbarkeit. Im Rahmen des ISMS werden alle auf die Ziele wirkenden Risiken identifiziert und bewertet. Für den Umgang mit den Risiken sind passende organisatorische und technische Maßnahmen implementiert. Nach Abstimmung mit den verantwortlichen Personenkreisen sind sie zu dokumentieren und in geeigneter Form zur Verfügung zu stellen.

Die Betrachtung weiterer Sicherheitsziele bzw. Grundwerte kann je nach Einsatzfall zu einer differenzierteren und ausgewogeneren Bewertung des Schutzbedarfes der Informationen führen. Insofern besteht grundsätzlich die Möglichkeit, weitere Sicherheitskriterien, unbeschadet etwaiger Schnittmengen oder Konkurrenz zwischen einzelnen Kriterien, heranzuziehen.

2.2 Grundsätze der Informationssicherheit

Die Belange der Informationssicherheit sind von Beginn an zu beachten, im Wesentlichen bei:

- der Planung und der Konzeption von IT-Verfahren
- ggf. der Entwicklung und der Einführung von IT-Verfahren
- dem Betrieb und der Pflege von IT-Verfahren
- der Dokumentation von vorhandenen IT-Verfahren
- der Beschaffung und der Beseitigung/Entsorgung von IT-Produkten
- der Nutzung von Diensten Dritter
- der Aus- und Weiterbildung der Mitarbeiter
- der Sensibilisierung der Mitarbeiter
- der Planung, Übung und Durchführung von Notfallplänen und im Krisenmanagement

2.2.1 Angemessenheit der IT-Sicherheitsmaßnahmen

Um Gefährdungen vorzubeugen sind organisatorische und technische Maßnahmen entsprechend der ISO/IEC 27001:2013 umzusetzen. Vorgänge mit einem besonders hohen Gefährdungspotential benötigen ggf. individuelle Betrachtungen und weiterergehende Maßnahmen.

Die Sicherheitsmaßnahmen sind entsprechend dem Unternehmensaufbau, der Personalausstattung und dem technischen Umfeld anzupassen. Dabei soll der finanzielle und technische Aufwand in einem ausgewogenen Verhältnis zu den tatsächlichen Risiken stehen.

2.2.2 Bereitstellung von Ressourcen

Zur Erreichung der IT-Sicherheitsziele werden durch die Geschäftsführung ausreichende finanzielle, personelle sowie zeitliche Ressourcen zur Verfügung gestellt. Sollten einzelne IT-Sicherheitsprozesse nicht finanzierbar sein, sind die IT-Sicherheitsmaßnahmen sowie die Art und Weise des IT-Betriebs zu überdenken und gegebenenfalls anzupassen.

2.2.3 Prinzip des informierten und sensibilisierten Mitarbeiters

Ein wesentliches Sicherheitsrisiko stellen bewusste sowie unbewusste sicherheitsgefährdende Handlungen der Anwender dar. Gezielte Sensibilisierung sowie Qualifizierung von Mitarbeitern sind Grundvoraussetzungen für die Informationssicherheit.

Anwender müssen ggf. über notwendige einschränkende IT-Sicherheitsmaßnahmen aufgeklärt und Verhaltensempfehlungen vermittelt werden. Die Beschäftigten des Unternehmens gewährleisten die notwendige und angemessene IT-Sicherheit durch verantwortungsvolles Handeln.

2.2.4 Sicherheit vor Verfügbarkeit

Wird die IT-Infrastruktur des Unternehmens angegriffen oder bedroht, können entsprechend dem Schutzbedarf vorübergehende Verfügbarkeitsbeschränkungen bei den betroffenen IT-Systeme vorgenommen werden. Dabei können in Abwägung der widerstreitenden Schutzgüter Einschränkungen beim Betrieb sowie im Komfort der Bedienung von IT-Systemen, insbesondere bei Netzübergängen in das Internet oder dem Anschluss in das Unternehmensdatennetz vertretbar sein.

2.2.5 Sicherung und Verbesserung (Kontinuität)

Ein kontinuierlicher Qualitätsverbesserungsprozess ist erforderlich, um neben der internen Optimierung ggf. auch eine übergreifende Vergleichbarkeit des erreichten Sicherheitsniveaus zu ermöglichen. Die regelmäßige Aktualisierung, Vervollständigung, Verbesserung und Wirksamkeitsprüfung der eingesetzten Sicherheitsmaßnahmen stellen einen permanenten Prozess dar.

Jeder Mitarbeiter ist angehalten, stetig, während seiner Arbeit Verbesserungsmöglichkeiten für das ISMS in Erwägung zu ziehen und dazu aktiv den ISMS-Beauftragten anzusprechen. Hierunter können organisatorische (z.B. aufgrund von Schwierigkeiten bei der Ausführung gegebener Verfahren) als auch technische (z.B. Einsatz neuer Technologien) Maßnahmen zählen.

2.3 Informationssicherheitsorganisation

Die Planungs-, Lenkungs- und Kontrollaufgaben, die erforderlich sind, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und diesen kontinuierlich umzusetzen, werden als Informationssicherheitsmanagementsystem (ISMS) bezeichnet. Es sind die unternehmensspezifischen Sicherheitsanforderungen und die Strukturierung bzw. Organisation der jeweiligen Geschäftsbereiche in ausreichendem Maße zu berücksichtigen.

Verantwortlich für die Umsetzung in den Geschäftsbereichen ist der ISMS-Beauftragte. Die Fachbereiche arbeiten loyal mit dem ISMS-Beauftragten zusammen, um die Ziele des ISMS erreichen zu können. Der ISMS-Beauftragte wird von der Geschäftsleitung bei der Umsetzung des ISMS durch entsprechende Ressourcen- und Budgetplanung angemessen unterstützt.

2.3.1 ISMS-Beauftragter

Für die Herbst Datentechnik GmbH ist ein verantwortlicher ISMS-Beauftragter bestellt, der über die Ergebnisse seines Aufgabenbereichs direkt an die Geschäftsleitung der Herbst Datentechnik GmbH berichtet. Die wesentlichen Aufgaben umfassen:

- Aufbau, Betrieb und Weiterentwicklung des ISMS und der Informationssicherheits-organisation innerhalb der Unternehmen
- Abstimmung der Informationssicherheitsziele mit den Zielen des Unternehmens
- Erstellung, Aktualisierung und Abstimmung der Leitlinie zur Informationssicherheit
- Begleitung und Hauptansprechpartner für jegliche Audits in Angelegenheiten des ISMS
- Dokumentation der ISMS-Prozesse
- Kontrolle der Umsetzung zu den IT-Sicherheitsstandards und den gesetzlichen Vorgaben zur IT-Sicherheit
- Erstellung von Berichten an die Geschäftsleitung des Unternehmens zum Umsetzungsstand ISMS
- Unterstützung bei der Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten
- Beratung der Geschäftsleitung und der Geschäftsbereiche in Belangen der Informationssicherheit, Initiierung und Steuerung von Angeboten für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit in Abstimmung mit dem Personalwesen
- Erstellung von Sicherheits- und Notfallvorsorgekonzepten im Zusammenhang IT

Dem ISMS-Beauftragten werden ausreichende Möglichkeiten einer qualifizierten Aus- und Fortbildung in Themen der Informationssicherheit gewährt. Zur Erfüllung der vorab genannten Aufgaben kann sich der Beauftragte unter seiner Kontrolle, geeigneter und qualifizierter Themenanbieter bedienen.

2.3.2 ISMS-Team

Zur einheitlichen Umsetzung der Informationssicherheitsorganisation und Abstimmung von Maßnahmen kann der ISMS-Beauftragte weitere Personen zur Beratung und für Zuarbeiten hinzuziehen, insbesondere

- die Fachexperten aus den Geschäftsbereichen
- die Geschäftsleitung
- den Datenschutzbeauftragten
- externe beratende Dienstleister zur Informationssicherheit
- Vertreter von Behörden

2.4 Aktualisierung

Die vorliegende Informationssicherheitsleitlinie wird entweder anlassbezogen oder mindestens alle 3 Jahre einer überprüfenden Revision unterzogen. Die Informationssicherheitsleitlinie wird dabei durch den ISMS-Beauftragten inhaltlich überprüft, im Bedarfsfall aktualisiert und danach zur Abstimmung gebracht.

2.5 Umsetzung der Leitlinie

Das für die Herbst Datentechnik GmbH und deren Sicherheitsziele erstellte ISMS tritt zum 01.10.2018 in Kraft.

Alle IT-Infrastrukturen, IT-Systeme und Anwendungen, welche nach dem Inkrafttreten dieser Leitlinie implementiert werden, sind unter anderem nach dem Sicherheitsstandard der ISO/IEC 27001:2013 und in Anwendung dieser Leitlinie umzusetzen.

2.6 Sanktionen

Art und Umfang von Sanktionen wegen Verletzung der Bestimmungen zum Schutz der Informationssicherheit sowie die Zuständigkeit für die Verfolgung ergeben sich aus den einschlägigen gesetzlichen Bestimmungen sowie den dazu erlassenen Richtlinien und Verordnungen.

Es ist besonders wichtig, Verstöße zu kommunizieren, um daraus zu lernen und alle Mitarbeiter zu sensibilisieren.

3. Verantwortlichkeiten/Dokumentation

3.1 Verantwortlichkeiten

Für die Umsetzung dieser Leitlinie ist neben dem ISMS-Beauftragten die Geschäftsleitung verantwortlich.

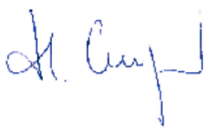
Weitere Verantwortlichkeiten und Aufgaben im Rahmen des ISMS ergeben sich aus der Rollenmatrix.

3.2 Dokumentation

Die Dokumentation richtet sich nach der Richtlinie Dokumentenlenkung.

4. Unterschriften

Berlin, den 01.10.2018



Geschäftsführung

Herbst Datentechnik GmbH