102/ls/Ku

15.01.2021

Stadtverwaltung
Frankenthal (Pfalz)

Leitlinie zur Informationssicherheit

nach BSI

Erstellt: 21.03.2012 Issle
Änderungen:
07.05.2012 Issle
24.05.2012 Issle
05.06.2012 Issle
27.04.2020 Kuhn
28.04.2020 Issle
12.08.2020 Kuhn
05.01.2021 Issle
15.01.2021 Issle

Verknüpfungen:
ISMS.1.A2
ISMS.1.A3

Leitlinie zur Informationssicherheit

Bezüglich der Informationssicherheit bei der Stadtverwaltung gilt folgende Leitlinie.

Stellenwert der Informationssicherheit

Da zur Erfüllung unserer Aufgaben eine Vielzahl von personenbezogenen Daten erhoben und gespeichert werden, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von höchster Bedeutung für die Betroffenen. Zur Aufgabenerfüllung der Verwaltung werden Zugriffe auf Informationen, wie Finanz-, Objekt- oder Prozessdaten benötigt. Langfristig sollen neben den heute schon digital gespeicherten Informationen alle in Papierakten vorliegenden Daten ebenfalls digitalisiert werden und größtenteils ausschließlich digital gespeichert werden. Damit werden alle strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können.

Übergreifende Ziele

Unsere Daten und unsere IT-Systeme werden in ihrer *Verfügbarkeit* so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (*Integrität*). Die Anforderungen an *Vertraulichkeit* haben ein überwiegend normales, an der Gesetzeskonformität orientiertes Niveau. Bei einzelnen Aufgaben werden jedoch auch sensible persönliche Daten gespeichert, so dass hohe Anforderungen an die Vertraulichkeit zu stellen sind.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen ebenso wie der Zugang zu personenbezogenen Daten durch Unbefugte verhindert werden.

Alle Mitarbeiter/innen halten die einschlägigen Gesetze (Datenschutzgesetz, sowie Spezialgesetze z.B. SGB) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für die Verwaltung sowie für die Mitarbeiter/innen durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter/innen und die Verwaltungsführung sind sich ihrer Verantwortung beim Umgang mit Informationen und der IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

Eine Umsetzung der Informationssicherheit auf Niveau der IT-Grundschutz-Vorgehensweise „Basis-Absicherung“ des Bundesamts für Informationssicherheit ist für uns selbstverständlich. Für ausgewählte Teile der Organisation ist als Vorgehensweise die Kernabsicherung gesetzlich verbindlich (vor allem Kfz-Wesen und Waffen-Register). In allen anderen Bereichen wird eine Standardabsicherung angestrebt.

Detailziele

Eine Sensibilisierung der Mitarbeiter für Informationssicherheit wird angestrebt.

Eine hohe Verfügbarkeit und Integrität, vor allem ein maximaler Schutz der Daten vor Verlust, sind grundsätzlich für alle Informationen und Leistungen der IT anzustreben.

Für die IT-Basisdienste, wie Dateiablage, Anmeldedienst, Datenbanken, oder Virenschutz usw., ohne die alle anderen IT-Leistungen nicht oder nur mit starken Einschränkungen zu erbringen sind, ist ein relativ hohes Schutzniveau bezüglich Backups der Verfügbarkeit und Integrität Grundvoraussetzung für den gesamten IT-Betrieb.

Das Finanzwesen CIP weist die höchste Nutzerzahl auf, so dass IT-Ausfälle Auswirkungen auf die Arbeitsfähigkeit einer hohen Zahl von Beschäftigten haben. Hier wird ein relativ hohes Schutzniveau bezüglich der Verfügbarkeit und Integrität angestrebt.

Gleiches gilt für Verfahren (z.B. VOIS, IKOL-KFZ) im Bereich der Bürgerdienste, da hier eine unmittelbare Außenwirkung besteht.

Da aufgrund unserer Aufgabenstellung als Kommunalverwaltung eine große Zahl personenbezogener und z.T. auch sensibler Daten gespeichert sind, ist dem Schutz dieser Daten vor Diebstahl, unbefugter Einsichtnahme oder Veränderung hohe Priorität einzuräumen.

Die Nutzung des Internets zur Informationsbeschaffung, zur Kommunikation und netzbasierter Dienste ist für uns selbstverständlich. E-Mail dient vielfach als Ersatz oder als Ergänzung anderer Bürokommunikationswege. Auch die Telefonie ist inzwischen als VoIP-Anwendung digitalisiert und erfordert entsprechenden Schutz. Durch geeignete Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wird eine Sicherheitsorganisation eingerichtet:

- IT-Sicherheitsbeauftragter – Die Funktion wird durch den Leiter der Abteilung Technikeinsatz, Herrn Issle, wahrgenommen.

- Datenschutzbeauftragter – Datenschutzbeauftragter ist der Leiter des Rechnungsprüfungsamtes. Da die Stelle z.Z. nicht besetzt ist, wird die Funktion des Datenschutzbeauftragten kommissarisch vom Leiter der Abteilung Technikeinsatz, Herrn Issle, übernommen.

- IT-Sicherheitsmanagement – Für das IT-Sicherheitsmanagement wird eine Arbeitsgruppe ITSM, bestehend aus dem IT-Sicherheitsbeauftragten, dem Datenschutzbeauftragten, einer technischen Sachbearbeitung von 102 und einer Verwaltungssachbearbeitung von 102 eingerichtet.

Die Arbeitsgruppe tagt mindestens vierteljährlich und berichtet direkt an den Oberbürgermeister.

Dem IT-Sicherheitsbeauftragten, dem Datenschutzbeauftragten und den Administratoren werden ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die festgelegten Informationssicherheitsziele zu erreichen.

Die Administratoren und der IT-Sicherheitsbeauftragte sind durch die IT-Benutzer/innen ausreichend in ihrer Arbeit zu unterstützen.

Der IT-Sicherheitsbeauftragte und der Datenschutzbeauftragte sind frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase informationssicherheitsrelevante Aspekte zu berücksichtigen.

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist die Bereichsleitung verantwortlich, es sei denn es wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf in Abstimmung mit dem ISB festlegt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertretungen ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden nach Möglichkeit auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und vermeidbare Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer/innen durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. vorzubeugen und gegebenenfalls vorübergehend in Kauf genommene Risiken, die im Normalbetrieb inakzeptabel wären, schnell zu eliminieren, muss auf sicherheitsrelevante Vorfälle und Situationen zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser informationstechnisches Ziel ist, auch bei einem Systemausfall kritische Arbeitsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Für die Abdeckung hoher finanzieller Risiken in Zusammenhang mit einen IT-Sicherheitsvorfall besteht eine Cyberversicherung.

Sofern IT-Dienstleistungen, die an externe Stellen als Auftragsdatenverarbeitung ausgelagert sind oder ausgelagert werden, sind in der Beauftragung die konkreten Sicherheitsanforderungen vorzugegeben. Das Recht auf Kontrolle ist festzulegen.

Die IT-Benutzer/innen werden regelmäßig in geeigneter Weise zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen angehalten.

Verbesserung der Sicherheit

Das Managementsystem der Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeiter/innen bekannt sind, ob sie umsetzbar und in den Arbeitsablauf integrierbar sind.

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter/innen sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

Stadtverwaltung Frankenthal (Pfalz) 18.03.21

A / 10 / 102 / DSB