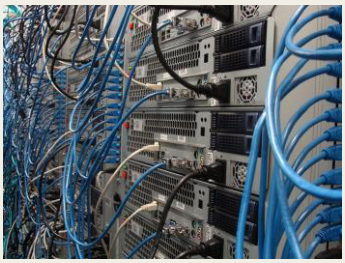
KGRZ

Informationssicherheitsleitlinie (ISLL) des KGRZ Koblenz



Dokument Information

Titel: ISLL

Version: 1.2
Datum: 19.12.2017
Ersteller: Detlev Reimann
Status: final

Verantwortlich: KGRZ-Leitung
Vertraulichkeit: öffentlich

Empfänger:
Team KGRZ
Werkausschuss
Security Management SV Koblenz

Speicherort:
Q:\Leitungsteam\10_Organisation\Dienstanweisungen\DA_KGRZ\ISLL-KGRZ

Informationssicherheitsleitlinie (ISLL) des KGRZ Koblenz

Inhalt

Informationssicherheitsleitlinie (ISLL) des KGRZ Koblenz

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	KGRZ übergreifende Leitlinie
Dokumententitel:	**Informationssicherheitsleitlinie des KGRZ ISLL**
Verantwortliche/r Autor/in:	Werkleitung KGRZ
Abgestimmt mit:	Informationssicherheitsbeauftragten des KGRZ
Dateiname:	ISLL.pdf
Inkrafttreten:	01.01.2018
Fassung vom	19.12.2017
Letzte Veröffentlichung am:	Januar 2018
Seitenzahl:	8
Vertraulichkeitsstufe:	**öffentlich**
Aktuelle Version:	1.2
Versionsfreigabe am:	19.12.2017
Freigegeben durch:	Werkleitung des KGRZ – Herr Andreas Sartorius

Änderungsnachweis

Versions-Nummer	Bearbeitungsstatus	In Kraft ab	Bearbeiter	Änderung/Bemerkung
1.0	erstellt	01.01.2018	Detlev Reimann	
1.1	geändert	01.01.2018	Andreas Sartorius	Redaktionelle Überarbeitung

Ergänzende Dokumente / Mitgeltende Unterlagen *

Titel des Dokuments Version	Aktuelle Fassung	Verantwortlicher Autor

* in der Tabelle sind alle Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, sprich in dem Dokument selbst explizit genannt werden oder darüber hinaus anzuwenden sind bzw. in diesem Zusammenhang von Relevanz sind.

1. Informationssicherheit im KGRZ

Das KGRZ hat die zentrale Aufgabe die informationstechnische Infrastruktur der Stadtverwaltung Koblenz bereit- und sicherzustellen. Insofern ordnet sich diese Aufgabe in die enorme Aufgabenvielfalt der Stadtverwaltung ein und unterstützt dabei den Prozess der zunehmenden Digitalisierung der Verwaltungsprozesse.

Weiterhin ist das KGRZ ein Dienstleister im Rahmen des ZIDKOR bzw. gegenüber Dritten und erfüllt in diesen Rahmen sicherstellende Aufgaben im kommunalen Umfeld.

Die Informationssicherheitsleitlinie (ISLL) des KGRZ ordnet sich daher den ISLL der Stadtverwaltung (primär) und des ZIDKOR unter und legt in diesem Zusammenhang grundsätzliche Rahmenbedingungen fest, welche das KGRZ zu verantworten hat.

Beim Einsatz der Informationstechnologie muss die Organisation des KGRZ darauf achten, dass die Sensibilität der ihr übertragenen und von ihr verarbeiteten Informationen mit der erforderlichen Sorgfalt Rechnung getragen wird. Die Informationssicherheit wird in zunehmendem Maße zu einer unverzichtbaren Grundlage für das Verwaltungshandeln, dem alle Beteiligten Vertrauen schenken sollen und können. Das KGRZ trägt somit eine grundsätzliche Verantwortung, Dienste mit „security by design" zu entwickeln und zu betreiben. Ein sehr wichtiger Bestandteil dieser Aufgabe ist, die Fachbereiche in dieser Entwicklung zu begleiten.

Es ist erforderlich, das Zusammenwirken von Fachanwendungen mit ihren Informationen, Aufgaben und Produkte sowie der zugehörigen Infrastruktur der Informationstechnik und den Kommunikationskanälen in ihrer Einheit zu betrachten. Die Informationssicherheit ist keineswegs eine technische Komponente sondern die Summe aller organisatorischen, personellen und technischen Maßnahmen, um festgelegte Ziele zu erreichen. Vertraulichkeit, Integrität und Verfügbarkeit der zu verarbeitenden Informationen sind ein hohes Gut.

Die Organisation des Informationssicherheitsmanagementsystems (ISMS) des KGRZ orientiert sich am IT-Grundschutz und den BSI-Standards 200-x (Rahmenwerk).

2. Geltungsbereich

Die ISLL gilt für den Verantwortungsbereich des KGRZ und der vom Rechenzentrum betriebenen Infrastruktur und IT-Systeme. Sie gilt auch für außerhalb des Dienstgebäudes eingerichtete Arbeitsplätze (mobile Arbeitsplätze/-geräte).

3. Sicherheitsziele

a) Unterstützung der Fachbereiche / Ämter bei der Wahrnehmung Ihrer Verantwortung hinsichtlich der Informationssicherheit in den jeweiligen Fachbereichen, in der Regel die Verfahrensverantwortlichen.
   Verfahrensverantwortlicher ist jede Person oder Organisationseinheit, der die Verantwortung für die Kontrolle von Produktion, Entwicklung, Pflege, Gebrauch und Sicherheit von Daten und der sie verarbeitenden Komponenten übertragen wurde.
b) Die Verfügbarkeit der IT-Systeme wird in einem solchen Umfang gesichert, dass Fehlfunktionen bzw. Unregelmäßigkeiten weitestgehend ausgeschlossen sind. Der erforderliche Umfang der Verfügbarkeit wird gemeinsam mit dem Verfahrensverantwortlichen festgelegt.

c) Die Anforderungen an Integrität und Vertraulichkeit der Daten ergeben sich aus den einschlägigen Gesetzen und vertraglichen Regelungen. Negative materielle und immaterielle Folgen für das KGRZ, die Verwaltung und die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden. Das beinhaltet verantwortungsbewusstes Handeln der Leitung und Mitarbeiter sowie eine sorgfältige Lösungsentwicklung und Betriebsvorbereitung.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Das bedarf einer sorgfältigen Prüfung in enger Zusammenarbeit mit den Fachbereichen und Ämtern. Schadensfälle mit hohen materiellen und immateriellen Auswirkungen sind inakzeptabel.

4. Informationssicherheitsmanagementsystems (ISMS)

Zur Erreichung der Informationssicherheitsziele ist eine Sicherheitsorganisation geschaffen. Die Verantwortung für die Organisation und den Prozess trägt die Werkleitung. Es ist ein Informationssicherheitsbeauftragter (ISB) bestellt worden. Er berichtet regelmäßig direkt an die Werkleitung und hat das Vortragsrecht.

Alle Mitarbeiter des KGRZ haben den ISB in seiner Arbeit fachlich ausreichend zu unterstützen. In Fragestellungen zur Informationssicherheit haben sich die Mitarbeiter an die Vorgaben des I-SiBe zu halten. Der ISB ist rechtzeitig in die Projekte und Ausschreibungsvorbereitungen einzubinden.

Den Mitarbeitern werden geeignete Ressourcen zur Verfügung gestellt, um Sachfragen der Informationssicherheit im Bereich ihrer Aufgaben zu berücksichtigen und zu klären. Informationssicherheit ist ein Bestandteil des Weiterbildungskonzeptes des KGRZ.

5. Grundlegende Maßnahmen

Für alle IT-Systeme und zu betreuenden Anwendungen wird ein verantwortlicher technischer Ansprechpartner benannt, der mit dem Verfahrensverantwortlichen der Fachbereiche zusammenarbeitet. Für alle diese Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können. Es besteht Dokumentationspflicht.

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 auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch geeignete Schutzmechanismen (Proxy-Strukturen, Firewalls, Einrichtung von demilitarisierten Zonen etc.) gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen Mitarbeiter im KGRZ 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. Es gibt ein Datensicherungskonzept.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Das Ziel des KGRZ ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

6. Verbesserung der Sicherheit

Das ISMS wird zweijährig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

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

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

7. Inkraftsetzung

Diese Leitlinie wird mit Wirkung vom 01. Januar 2018 in Kraft gesetzt

Koblenz, den 19.12.2017

Werkleitung KGRZ Koblenz