Kreis Rendsburg-Eckernförde
Der Landrat

Rendsburg, 31.01.2019

Mitteilungsvorlage Federführend: FD 1.2 IT-Service	Vorlage-Nr: VO/2015/757 Status: öffentlich Datum: 28.12.2015 Ansprechpartner/in: Rix, Svend Bearbeiter/in: Rix, Svend
Mitwirkend:	**öffentliche Mitteilungsvorlage**

Informationssicherheitsleitlinie für den Kreis Rendsburg-Eckernförde

Beratungsfolge:

Status	Gremium	Zuständigkeit
	Hauptausschuss	Kenntnisnahme

1. Begründung der Nichtöffentlichkeit: Entfällt

2. Sachverhalt:
Der Fachdienst 1.2 richtet die Informationssicherheit der Kreisverwaltung insbesondere nach der Prüfung des LRH im Jahre 2013 neu aus. Diese Aufgabe und das Vorgehen orientieren sich dabei an den geltenden Standards des Bundesamtes für Sicherheit in der Informationssicherheit (BSI). Hierzu bedarf es nach dem BSI-Standard 100-1 dem Aufbau eines wirksamen Managementsystems für Informationssicherheit.

Ein Grundpfeiler hierfür ist die Entwicklung und Inkraftsetzung einer Informations-sicherheitsleitlinie für die gesamte Kreisverwaltung bzw. alle Nutzerinnen und Nutzer der Informationstechnik der Kreisverwaltung. Daher gehören zum Adressatenkreis auch die Kreistagsabgeordneten und die bürgerlichen Mitglieder in den Ausschüssen.

Der Informationssicherheitsbeauftragte des Kreises hat hierzu eine den Regelungen des BSI entsprechende Leitlinie (Anlage) für die Kreisverwaltung entwickelt. Sie bildet den ersten Schritt zur Definition und Ausgestaltung eines (IT-)Sicherheitsprozesses innerhalb der Kreisverwaltung. Mit ihr werden die Sicherheitsstrategie, die Sicherheitsmaßnahmen und das Bekenntnis der Behördenleitung zur Informationssicherheit als gesamtheitlichem Sicherheitsprozess definiert.

Sie entwickelt keine unmittelbare Wirkung auf den in der Leitlinie genannten Adressatenkreis, sondern bildet den Rahmen für die Weiterentwicklung der Informationssicherheit der Kreisverwaltung.

Finanzielle Auswirkungen:
Keine

Anlage/n:

Kreis Rendsburg-Eckernförde
Der Landrat

Informationssicherheitsleitlinie

für die

Kreisverwaltung Rendsburg-Eckernförde

Bezeichnung des Dokumentes:	Informationssicherheitsleitlinie für die Kreisverwaltung Rendsburg-Eckernförde
Verantwortliche Stelle:	Micha Mark Knierim, Informationssicherheitsbeauftragter Telefon 04331 / 202-174 E-Mail: michamark.knierim@kreis-rd.de
Version:	1.1 vom 27. Oktober 2015
Dokumentenstatus:	öffentlich

Inhaltsverzeichnis

1 Einleitung

Ausgangssituation

Bei der Einführung jedes Informations- und Kommunikationstechnik- (IT)-Verfahrens bzw. jeder IT-Anwendung stellt sich die Frage nach der Sicherheit und dem Schutz der Daten, die mit ihnen verarbeitet werden sollen. Hundertprozentige Sicherheit ist nie zu erreichen, weder im täglichen Leben noch bei der Informationssicherheit. Das erreichbare Sicherheitsniveau wird bestimmt vom maximalen finanziellen und personellen Aufwand, den die jeweilige Organisationseinheit für ihre Sicherheit betreiben kann bzw. will. Das vorliegende Dokument enthält Leitaussagen zur Informationssicherheitsstrategie der Kreisverwaltung Rendsburg-Eckernförde, um die zu verfolgenden Informationssicherheitsziele und das angestrebte Informationssicherheitsniveau für alle Mitarbeiterinnen und Mitarbeiter zu dokumentieren.

Die Informationssicherheitsleitlinie ist Teil der IT-Gesamtkonzeption für die Standard-IT der Kreisverwaltung Rendsburg-Eckernförde, welche neben den Fachkonzepten auch Sicherheitskonzepte und die Dokumentation der übergreifenden Sicherheitsorganisation umfasst. Diese wird durch den Fachdienst 1.2 (IT-Service) gesteuert.

2 Festlegung des Geltungsbereichs

Diese Informationssicherheitsleitlinie gilt für die Informationstechnik der Verwaltung des Kreises Rendsburg-Eckernförde. Sie trifft für alle Organisationseinheiten (Landrat, Fachbereiche, Stabstellen, Fachdienste, Personalrat, Gleichstellungsbeauftragte, Schwerbehindertenvertretung) und damit für alle Mitarbeiterinnen und Mitarbeiter der Kreisverwaltung Rendsburg-Eckernförde grundsätzliche Regelungen zur Informationssicherheit. Darüber hinaus gilt sie für alle Nutzerinnen und Nutzer der IT-Infrastruktur und der damit verbundenen Informationstechnik des Kreises Rendsburg-Eckernförde (u. a. Mitglieder des Kreistages und bürgerliche Mitglieder in den Ausschüssen).

Der Datenschutz ist kein direkter Bestandteil dieser Leitlinie. Dieser ist gesondert in der „Dienstvereinbarung über den Datenschutz“ geregelt, wobei Überschneidungen möglich und unvermeidbar sind.

Unter Informationstechnik (IT) werden alle technischen Systeme verstanden, die dazu bestimmt sind, Informationen und Daten zu verarbeiten, zu erfassen oder zu übertragen, soweit diese zur Abwicklung der Geschäftsprozesse der Verwaltung benötigt werden und nicht ausschließlich der Steuerung von BTA (betriebstechnische Anlagen wie Klimaanlagen, Fahrstühle, Heizungs-, Wasser- und Stromversorgung von Gebäuden pp.) dienen.

3 Rechtliche Grundlagen

Es gelten die Vorschriften des Landesdatenschutzgesetzes SH, insbesondere die §§ 5 und 6 LDSG (Maßnahmen zur Datensicherheit) und § 8 Abs. 2 LDSG (Verfahrensverantwortung für gemeinsame Verfahren).

Aus den Mindestanforderungen der Rechnungshöfe[1] leiten sich unmittelbar Anforderungen zur Einrichtung eines Informationssicherheitsmanagements und zur Umsetzung notwendiger Maßnahmen zur Informationssicherheit unter Anwendung von Standards und der Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) ab.

Darüber hinaus empfiehlt die Leitlinie für Informationssicherheit des IT-Planungsrats vom 19.02.2013 den Kommunen zur Erstellung einer Informationssicherheitsleitlinie und zum Aufbau eines Sicherheitsmanagements.

4 Stellenwert der Informationsverarbeitung

Jegliche Aufgabenerfüllung ist ohne Informationstechnik (IT) heute praktisch nicht mehr möglich. Informationsverarbeitung spielt eine Schlüsselrolle für die Handlungsfähigkeit der Kreisverwaltung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch IT maßgeblich unterstützt. Zunehmend werden auch Kernaufgaben der Verwaltung ausschließlich IT-gestützt abgewickelt; dies stellt zusätzliche Anforderungen an die Sicherheit der eingesetzten Informationstechnik.

Alle Mitarbeiterinnen und Mitarbeiter, insbesondere alle Führungskräfte sind sich ihrer Verantwortung im Umgang mit IT bewusst und unterstützen die Informationssicherheitsstrategie nach besten Kräften.

Sie werden durch geeignete Maßnahmen, u.a. durch Veröffentlichung der Konzeptlage, Informationsveranstaltungen und Schulungen, für die Belange der Informationssicherheit sensibilisiert.

Die Qualität der Umsetzung von technischen, organisatorischen und personellen Maßnahmen im Rahmen eines Sicherheitsprozesses und insbesondere die Akzeptanz gegebenenfalls notwendiger funktionaler Einschränkungen sind maßgeblich von der Unterstützung der Leitungsebene abhängig. Ohne diese Unterstützung bleiben Maßnahmen oft unwirksam.

Mit dieser Informationssicherheitsleitlinie bekennt sich die Behördenleitung zu ihrer Verantwortung für Informationssicherheit. Aus diesem Grund erlässt sie eine für die gesamte Kreisverwaltung verbindliche Informationssicherheitsleitlinie als Bestandteil ihrer Sicherheitsstrategie.

Selbst wenn einzelne Aufgaben im Rahmen des Informationssicherheitsprozesses an Personen oder Organisationseinheiten delegiert werden, welche für die Umsetzung zuständig sind, verbleibt die Gesamtverantwortung bei der Behördenleitung.

[1] https://www.bundesrechnungshof.de/de/veroeffentlichungen/broschueren/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik

5 Festlegung von Sicherheitszielen

Ziel ist die Umsetzung einer nach gesetzlichen und vertraglichen Vorgaben ordnungsgemäßen Datenverarbeitung durch Bereitstellung einer datenschutzfreundlichen und technisch sicheren Infrastruktur zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen jeglicher Art.

Informationssicherheitsmaßnahmen müssen sich an den schützenswerten Informationen und IT-Systemen orientieren. Sie müssen daneben aber auch in einem wirtschaftlich vertretbaren Verhältnis zum Wert dieser schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit Auswirkungen auf die informationelle Selbstbestimmung oder hohen finanziellen Auswirkungen müssen verhindert werden.

Für die Entwicklung und den Betrieb der IT-Infrastruktur der Kreisverwaltung gelten daher folgende Sicherheitsziele:

- Schutz vertraulicher Daten aller Beteiligten
- Gewährleistung der Verfügbarkeit der Daten und der Informationssysteme
- Gewährleistung der Integrität, Vollständigkeit und Authentizität der Daten
- Sicherstellung der Kontinuität der Arbeitsabläufe
- Sicherstellung der Verfügbarkeit kritischer Geschäftsprozesse
- transparente und nachvollziehbare Gestaltung der Datenverarbeitungsprozesse
- Gewährleistung einer „datenschutzfreundlichen Infrastruktur“
- Umsetzung der datenschutzrechtlichen Anforderung bezüglich Transparenz, Nicht-Verkettbarkeit, Betroffenenrechte und Zweckbindung

6 Sicherheitsstrategie

Das angestrebte Sicherheitsniveau wird durch folgende Sicherheitsstrategie erreicht:

- Es werden Regelungen für die Aufbau- und Ablauforganisation innerhalb der Kreisverwaltung geschaffen.
- Die zu ergreifenden Sicherheitsmaßnahmen werden in einer modularen Sicherheitskonzeption festgelegt.
- Ein Integriertes Sicherheitsmanagement-System (ISMS Kreis RD-ECK) wird etabliert und kontinuierlich weiterentwickelt (s.7).
- Es erfolgt eine den Regelungen des § 17 LDSG entsprechende Auftragsdatenverarbeitung. Sofern IT-Dienstleistungen an externe Stellen (z.B. Dataport) ausgelagert werden, werden konkrete vertragliche Regelungen getroffen. Dabei werden Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben sind Informationssicherheitskonzepte mit konkreten Maßnahmenvorgaben zu erstellen.
- Die für die Fachverfahren eingesetzten Informationssysteme werden voneinander ablauforganisatorisch und systemtechnisch in Entwicklung und Betrieb getrennt.
- In einem Berechtigungskonzept wird ein revisionsfähiges Verfahren für die Vergabe von Berechtigungen zur Nutzung der in der Kreisverwaltung eingesetzten Informationssysteme dokumentiert.
- Die für die Informationssicherheit zuständigen Mitarbeiterinnen und Mitarbeiter werden kontinuierlich geschult.
- Die Mitarbeiterinnen und Mitarbeiter der Kreisverwaltung werden auf die Einhaltung der für die Informationssicherheit des Verfahrens relevanten Gesetze, Verordnungen, Richtlinien, Anweisungen und vertraglichen Vereinbarungen verpflichtet und über die dienst- bzw. arbeitsrechtlichen Folgen von Verstößen informiert.
- Es wird eine praxis- und rechtskonforme Dokumentation über die eingesetzten Informationssysteme erstellt und aktuell gehalten.
- Die in den Sicherheitskonzepten festgelegten Maßnahmen werden regelmäßig durch den Informationssicherheitsbeauftragten überprüft.
- Es wird eng mit dem Datenschutzbeauftragten der Kreisverwaltung zusammengearbeitet.
- Grundsätzlich wird nach den BSI-Standards vorgegangen.

- Sofern möglich, sollen durch das BSI bzw. durch das ULD zertifizierte Produkte und Systeme bevorzugt eingesetzt werden[2].

7 IT-Sicherheitsorganisation

Das Herstellen und Erhalten des Informationssicherheitsniveaus ist eine Aufgabe aller Personen, die an der Basisinfrastruktur beteiligt sind oder dessen IT-Ressourcen nutzen.

7.1 Informationssicherheitsbeauftragter und -Management

Es wird ein Integriertes Informationssicherheitsmanagement (ISMS Kreis RD-ECK) eingerichtet, das aus dem Sicherheitsverantwortlichen (nachfolgend Informationssicherheitsbeauftragter, bzw. ISB genannt), dem Datenschutzbeauftragten und dem IT-Leiter besteht. Der Informationssicherheitsbeauftragte ist gem. den unter Ziff. 3 benannten Anforderungen zu bestellen.

Dem ISB werden von der Behördenleitung ausreichende personelle, finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um die Informationssicherheitsziele zu erreichen und um sich regelmäßig weiterzubilden und zu informieren. Der ISB wird durch die IT-Benutzerinnen und Benutzer in seiner Arbeit unterstützt. Er ist frühzeitig in alle Prozesse einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

7.2 Behördliche Datenschutzbeauftragte

Der Informationssicherheitsbeauftragte arbeitet eng mit dem gem. § 10 LDSG ernannten behördlichen Datenschutzbeauftragten zusammen. Er ist in das ISMS Kreis RD-ECK einzubinden.

7.3 Mitarbeiterinnen und Mitarbeiter

Die Mitarbeiterinnen und Mitarbeiter sind dafür verantwortlich, dass die sie betreffenden Sicherheitsmaßnahmen in ihrem Aufgabenbereich umgesetzt werden. Unterstützt durch sensibilisierende Schulung und eine angemessene Betreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten Sicherheitsvorfälle von innen und außen vermeiden. Sicherheitsrelevante Ereignisse sind dem Informationssicherheitsbeauftragten umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können. Die IT-Benutzerinnen und Benutzer haben sich in sicherheitsrelevanten Fragestellungen, die die Gesamtsicherheit der IT-Basisinfrastruktur betreffen, an die Anweisungen aus dem ISMS Kreis RD-ECK zu halten.

[2] Datenschutz-Gütesiegel nach §4 Abs. 2 LDSG; https://www.datenschutzzentrum.de/guetesiegel

7.4 Verfahrensverantwortliche

Die in den Fachbereichen zuständigen Personen für Daten, Informationen und Verfahren entscheiden, wer in welchem Umfang Zugriff auf das jeweilige System hat. Wenn sie Vorgaben zur Informationssicherheit formulieren, haben sie auch den angemessenen Schutzbedarf, die Finanzierbarkeit bzw. Wirtschaftlichkeit abzuwägen.

8 Sicherheitsmaßnahmen

Für die betriebene und geplante Informationstechnik sind Informationssicherheitskonzepte zu erstellen. Diese Informationssicherheitskonzepte beinhalten eine Schutzbedarfsfeststellung, eine Sicherheitsanalyse und die darauf folgende Umsetzung der nach BSI-Grundschutz erforderlichen Maßnahmen. Weiteres ist in den jeweiligen Richtlinien, Dienstvereinbarungen oder Dienstanweisungen zu regeln.

9 Bekanntgabe

Diese Informationssicherheitsleitlinie ist öffentlich. Sie wird allen Mitarbeiterinnen und Mitarbeitern in geeigneter Weise bekannt gegeben.

10 Revision

Diese Informationssicherheitsleitlinie soll entsprechend den Vorgaben der BSI-Standards in regelmäßigen Abständen, möglichst alle zwei Jahre, auf ihre Aktualität und Wirksamkeit überprüft werden.

11 Inkrafttreten

Diese Informationssicherheitsleitlinie tritt mit ihrer Unterzeichnung in Kraft.

Rendsburg,

Dr. Rolf-Oliver Schwemer
L a n d r a t