Ev.-Luth. Kirchenkreis
Rantzau-Münsterdorf

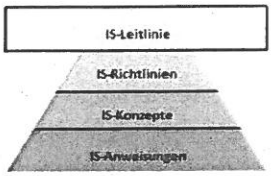
Leitlinie

zur Informationssicherheit

Souren Nikogosian

03.04.2019

Der Kirchenkreisrat verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil seiner Strategie



Ev.-Luth. Kirchenkreis Rantzau-Münsterdorf

Leitlinie zur Informationssicherheit

Stand 04-2019

Typ	Leitlinie
Titel	Leitlinie zur Informationssicherheit
Version	0.1
Gültig für	Ev.-Luth. Kirchenkreis Rantzau-Münsterdorf
Abgestimmt mit	Fachdienst IT, Datenschutzbeauftragte, KKR, MAV (nach KKR Beschluss)
Ansprechpartner	Souren Nikogosian, Tel.: +4941212625614
Pflegeverantwortlicher Bereich	Informationssicherheit

Inhalt

Versionierung

Version	Bearbeiter	Datum	Inhalt	Review Partner
0.1	Souren Nikogosian	11.03.2019	Ersterstellung	Alexandra Magens Karsten Arp Ralf Fischer

1 Stellenwert der Informationsverarbeitung

Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf unser Tagesgeschäft nicht zusammenbrechen.

Vernetzte Computersysteme sind durch Dritte von innen und von außen angreifbar. Zusätzliche Risiken bestehen durch die Nutzung von mobilen Arbeitsplätzen, durch höhere Gewalt, organisatorische Mängel, Fehlbedienung, technisches Versagen und vorsätzliche Handlungen wie Diebstahl.

Ziel der IT-Sicherheit ist es, Missbrauch, Risiken und Gefahren zu erkennen, Maßnahmen zur Eindämmung zu beschreiben und diese wirksam umzusetzen. Eine Umsetzung der Maßnahmen bedeutet in der Regel auch eine Einschränkung bei der Bedienbarkeit und Funktionalität und es muss laufend zwischen unterschiedlichen Interessen abgewogen werden. Kompromisse, die dabei einzugehen sind, müssen von der Leitung und jedem*r Mitarbeitenden getragen werden.

Seit Mitte 2015 gilt die Verordnung der EKD zur Sicherheit in der Informationstechnik, kurz: „IT-Sicherheitsverordnung – ITSVO-EKD". Die Umsetzung der ITSVO ist nach DSG-EKD - § 27 Absatz 6 Satz 2 für jede kirchliche Stelle verpflichtend.

Nach § 6 der ITSVO-EKD können Durchführungsbestimmungen zu der Verordnung und ergänzende Bestimmungen zur IT-Sicherheit erlassen werden.

Als Kirchenkreis verarbeiten wir eine Vielzahl von (auch personenbezogenen) Daten, um unsere Aufgaben und Pflichten gegenüber unseren Kunden, Vertragspartnern, Dienstleistern, Behörden und sonstigen Dritten zu erfüllen. Dabei verarbeiten wir auch Daten, die einen höheren Schutzbedarf aufweisen und die vor der unberechtigten Kenntnisnahme durch Dritte besonders zu schützen sind. Die Sicherheit der Informationsverarbeitung spielt daher eine Schlüsselrolle für unsere Aufgabenerfüllung. Diese Leitlinie soll die Sicherheitsstrategie, die Sicherheitsorganisation und die Sicherheitsziele in übersichtlicher Form darstellen.

2 Zweck

Diese Leitlinienempfehlung stellt bewusst auf Informationssicherheit und nicht ausschließlich auf IT-Sicherheit ab. Ziel ist der Schutz sämtlicher im Kirchenkreis verarbeiteter schutzbedürftiger Informationen unabhängig vom Trägermedium, neben Computerdaten sind somit zum Beispiel auch Papierdaten gemeint.

Definition Informationssicherheitsmanagementsystem (ISMS):

Das ISMS ist die Gesamtheit von Mitarbeiter*Innen, Prozessen und Regeln innerhalb einer Organisation, welche dazu dient, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Der Aufbau eines

ISMS sollte anhand einer bewährten und anerkannten Methode erfolgen. Am Bekanntesten ist hier die Grundschutzmethodik des BSI (Bundesamt für Sicherheit in der Informationstechnik).

3 Begriffseinführung

Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein akzeptierbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen.

Dabei bedeuten:

Vertraulichkeit: Vertrauliche Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang, sowie die Daten über den Sende- und Empfangsvorgang.

Integrität: Der Begriff der Integrität bezieht sich sowohl auf Informationen, Daten als auch das gesamte IT-System. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Zum anderen bezieht sich der Begriff Integrität auch auf IT-Systeme, da die Integrität der Informationen und Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden kann.

Verfügbarkeit: Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

4 Geltungsbereich

Diese Leitlinie gilt zunächst für das Kirchliche Verwaltungszentrum in Itzehoe (Haus der Kirche), Kirchliche Zentrum Elmshorn, Kirchenkreisarchiv in Stellau und Propstenhaus in Itzehoe.

5 Übergreifende Ziele

Unsere Daten und unsere IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer **Verfügbarkeit** so gesichert, dass die zu erwartenden Stillstand-Zeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel. Die Anforderungen an **Vertraulichkeit** haben ein normales, an Gesetzeskonformität orientiertes Niveau.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Alle Mitarbeiter*innen des Kirchenkreises halten die einschlägigen Gesetze, Regelungen zum Datenschutz und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für den Kirchenkreis sowie für die Mitarbeiter*innen durch Gesetzesverstöße sind zu vermeiden.

Als Straftaten kommen insbesondere in Betracht:

das unbefugte Verschaffen von Daten anderer, die nicht für den/die Mitarbeiter*in bestimmt und die gegen den unberechtigten Zugang besonders gesichert sind,

das Schädigen fremden Vermögens durch unrichtiges Gestalten eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugtes Verwenden von Daten oder durch unbefugtes Einwirken auf den Ablauf eines Programms,

das rechtswidrige Löschen, Verändern, Unterdrücken und Unbrauchbarmachen von Daten,

das unbefugte Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers oder

strafbewehrte Verstöße gegen das Datenschutzgesetz der EKD oder das Bundesdatenschutzgesetz.

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

Verstöße gegen die Informationssicherheit sind unverzüglich dem zuständigen Beauftragten für Informationssicherheit zu melden.

6 Detailziele

Verspätete oder fehlerhafte Entscheidungen der Leitungsorgane können weitreichende Folgen nach sich ziehen. Daher ist, bei wichtigen Entscheidungen, der Zugriff auf aktuelle Daten wichtig. Für diese Informationen ist ein erhöhtes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.

Die Datenschutzgesetze und die Interessen unserer Mitarbeiter*innen verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kunden und Geschäftspartner.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

7 Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet. Es ist ein*e Informationssicherheitsbeauftragte benannt worden. Der/die Informationssicherheitsbeauftragte berichtet in seiner/ihrer Funktion direkt an den Kirchenkreisrat.

Dem/der Informationssicherheitsbeauftragten*r und den Administratoren werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Management festgelegten Informationssicherheitsziele zu erreichen.

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

Der/die Informationssicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für die/den Datenschutzbeauftragte*n.

Die IT-Benutzer*innen haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen der/des Informationssicherheitsbeauftragten zu halten.

Es wurde ein*e Datenschutzbeauftragte*r bestellt. Der/die Datenschutzbeauftragte hat ein ausreichend bemessenes Zeitbudget für die Erfüllung ihrer/seiner Pflichten zur Verfügung. Der/die Datenschutzbeauftragte ist angehalten, sich regelmäßig weiterzubilden.

8 Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter*innen 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 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 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.

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. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellen wir ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.

IT-Benutzer*innen nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Der Kirchenkreisrat unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

9 Umsetzung

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte und detaillierter Regelungen und Dienstanweisungen zur Informationssicherheit.

10 Verbesserung der Sicherheit

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

Die Informationssicherheit ist systematisch und umfassend an die technischen und rechtlichen Entwicklungen anzupassen, damit eine möglichst optimale Sicherheitsfunktionalität erreicht wird.

Die umzusetzenden Lösungen sollen praxistauglich und ausreichend komfortabel gestaltet werden, damit sie von den Mitarbeitenden auch in der täglichen Arbeit nicht als belastend, sondern als sinnvoll akzeptiert werden.

Die Anwender*innen haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen der/den Informationssicherheitsbeauftragten zu halten.

Der Kirchenkreisrat 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 Informationssicherheitstechnik zu halten.

Diese Leitlinie tritt am 01.06.2019 in Kraft.

Itzehoe, 17/6/19
Ort, Datum

Dr. Thomas Bergemann, Propst
Vorsitzender des Kirchenkreisrates

Mitglied des Kirchenkreisrates