Evangelische Landeskirche in Baden

Evangelischer Oberkirchenrat

EVANGELISCHE LANDESKIRCHE IN BADEN

IT-Sicherheitskonzept

INHALTSVERZEICHNIS

1 Dokumenteninformation

1.1 Dokumentendaten

Typ	Dokumentenverantwortlicher*in	Version
Leitlinie	Informationssicherheitsbeauftragter (ISB)	Siehe Info im SharePoint

1.2 Dokumentenhistorie

Letzte Änderung	Bearbeiter*in	Status
2024-02-01	Y.Lackus	In Arbeit

1.3 Beteiligte Personen

Name	E-Mail-Adresse	Telefonnummer	Rolle
Robin Leitner	Robin.leitner@secudor.de	0151-56397545	Externer Berater
Yannick Lackus	Yannick.Lackus@ekiba.de	0721-9175-578	Projektmanagement
Timo Geiss	Timo.Geiss@ekiba.de	0721-9175-780	Abteilungsleitung
Alfred Ernst	Alfred.Ernst@ekiba.de	0721-9175-603	DSB / ISB

2 ZIELSETZUNG DES IT-SICHERHEITSKONZEPTS

2.1 Rahmenbedingungen / Ausgangslage

Für die Handhabung und den Schutz von Informationen in der Evangelischen Kirche in Baden (EKIBA) orientiert sich die EKIBA an dem internationalen Standard ISO 27001, welcher die Anforderungen für Informationssicherheits-Managementsysteme (ISMS) festlegt. Dies stellt eine gezielte Entscheidung der EKIBA dar, die von der allgemeinen Empfehlung der ITSVO-EKD (Informations- und Telekommunikations-System-Verordnung der Evangelischen Kirche in Deutschland) abweicht. Während die ITSVO-EKD generell den BSI-Standard für Informationssicherheit nahelegt, hat sich die EKIBA für die Anwendung der ISO 27001 entschieden. Ergänzend dazu spielt im kirchlichen Kontext auch das DSG-EKD (Datenschutzgesetz der Evangelischen Kirche in Deutschland) eine Rolle. Obwohl diese Norm primär Datenschutzbelange behandelt, enthält sie ebenfalls wichtige Aspekte, die für die Sicherheit von Informationen relevant sein können.

2.2 Zielsetzung und Vorgehensweise

Die primäre Zielsetzung des IT-Sicherheitskonzepts ist die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit aller informationsverarbeitenden Systeme und Prozesse. Dies umfasst den Schutz sensibler Daten vor unbefugtem Zugriff, die Sicherstellung der Korrektheit und Vollständigkeit der Daten sowie die Gewährleistung, dass die IT-Dienste jederzeit den Benutzern zur Verfügung stehen. Durch die Anwendung der ISO 27001 und die Berücksichtigung des DSG-EKD soll ein umfassendes

Informationssicherheits-Managementsystem etabliert werden, das sowohl internationale Best Practices als auch kirchenspezifische Datenschutzanforderungen integriert.

Zur Erreichung dieser Zielsetzung wird folgende Vorgehensweise gewählt:

- Durchführung einer initialen Bestandsaufnahme aller informationsverarbeitenden Systeme und Prozesse innerhalb der EKIBA, um den aktuellen Sicherheitsstatus zu ermitteln.
- Identifikation und Bewertung aller relevanten Sicherheitsrisiken, die sich aus der Verarbeitung von Informationen ergeben.
- Entwicklung und Implementierung eines maßgeschneiderten Sicherheitskonzepts, das auf den identifizierten Risiken basiert und geeignete Sicherheitsmaßnahmen zur Risikominderung vorsieht.
- Regelmäßige Überprüfung und Anpassung des Sicherheitskonzepts an veränderte Rahmenbedingungen oder neue Sicherheitsbedrohungen, um ein kontinuierliches Schutzniveau sicherzustellen.

2.3 Methodik und Werkzeuge

Die Methodik zur Entwicklung und Umsetzung des IT-Sicherheitskonzepts basiert auf dem Plan-Do-Check-Act (PDCA)-Zyklus, das für die stetige Verbesserung der Informationssicherheit sorgt. Als Grundlage dient die Methodik der ISO 27001:2022 sowie die Werkzeuge der ISO27002:2022. Im Rahmen der Gefährdungsanalyse werden die Gefährdungen des BSI „Elementare Gefahren“ herangezogen.

3 INFORMATIONSVERBUND

3.1 Definition des Informationsverbund

Der Informationsverbund unterstützt die Geschäftsprozesse zur Erbringung der seelsorgerischen Beratungsdienstleistungen durch die EKIBA. Zur Erbringung ihrer Leistungen benötigt die EKIBA unterschiedlichste IT-Systeme. Primär werden IT-Systeme mit einem Windows-Betriebssystem eingesetzt. Im Rahmen der Tätigkeiten werden Notebooks verwendet, mit denen, bei einem mobilen Einsatz vor Ort, die Einwahl über eine Webanwendung oder Citrix-Verbindung auf die internen Systeme der Organisation erfolgt. Für die Bürokommunikation wurde eine E-Mail-Infrastruktur mit Hilfe der M365 Suite implementiert. Im Rahmen der Projekttätigkeiten wird auf Serversysteme zugegriffen, welche sich in einem Rechenzentrum am Standort Karlsruhe befinden. Die bereitgestellten Serversysteme werden in einer Virtualisierungsinfrastruktur abgebildet. Entsprechend der Funktionalität und des Schutzbedarfs erfolgt eine Aufteilung der IT-Systeme in unterschiedliche Netze.

3.2 Kritische Fachaufgaben und -verfahren

Die kritische Fachaufgaben und -verfahren gliedern sich in verschiedene Kernbereiche, die für die reibungslose Funktion des Gesamtsystems unerlässlich sind.

Zu diesen zählen:

- **Virtualisierungslösung für Applikationen**: Dies bezieht sich auf die Implementierung und Verwaltung von Softwarelösungen, die es ermöglichen, Anwendungen effizient und sicher auf virtualisierten Plattformen zu betreiben.
- **Meldewesen**: Dies umfasst die systematische Erfassung, Verarbeitung und Weiterleitung relevanter Informationen und Daten, die für regulatorische oder kirchliche Zwecke erforderlich sind.
- **Gottesdienstverwaltung**: Dies betrifft die Organisation und Koordination aller Aspekte, die mit der Planung und Durchführung von Gottesdiensten zusammenhängen.
- **Infrastruktur**:
  - *CMDB*: Dieses Tool dient der Verwaltung der IT-Infrastruktur, einschließlich der Erfassung und Dokumentation von IT-Assets.
  - *Entra ID*: Ein Dienst für die Identitäts- und Zugriffsverwaltung, der sicherstellt, dass nur autorisierte Personen Zugriff auf wichtige Systeme und Daten haben.
  - *Desktop-Virtualisierung*: Diese Tools sind entscheidend für die Bereitstellung und das Management von Anwendungen und Ressourcen in einem Netzwerk.
- **Finanzsteuerung**:
  - *Finanzbuchhaltung, elektronischer Belegworkflow, SF Buchungsplan, SF Kirchensteuerkappung*: Diese Systeme sind zentral für die Verwaltung und Steuerung der Finanzen, einschließlich Buchhaltung, Budgetierung und spezifischer kirchlicher Finanzvorgänge.
- **Ticketsystem**: Ein wichtiges Tool für das Management von Kommunikation und Arbeitsabläufen innerhalb der Organisation.
- **Personalverwaltung**:
  - *Personalwirtschaftssystem und digitale Personalakte*: Eine Softwarelösung für die Verwaltung von Personalangelegenheiten.
  - *Gehaltsabrechnung*: Ein Gehaltsabrechnungssystem ist ein System, das für die Abrechnung von Gehältern und Reisekosten unerlässlich ist.
  - *Self-Service-Portale:* Softwarelösung zur Erfassung von Reisekosten, Abruf von Gehaltsmitteilungen und anderen Dokumenten
- **Dokumentenmanagement**:
  - *Sharepoint*: Ein zentrales Tool für das Speichern, Teilen und Verwalten von Dokumenten innerhalb der Organisation.

Diese Fachaufgaben und -verfahren sind entscheidend für die Aufrechterhaltung der operativen Effizienz und Sicherheit der Organisation und bedürfen daher einer kontinuierlichen Überwachung und Pflege.

3.3 Beschreibung der Schnittstellen mit externen Partnern/Dienstleistern

- *Microsoft im Bereich Dokumentenablage* Microsoft ist verantwortlich für die Bereitstellung der Plattform und Tools für das Dokumentenmanagement, einschließlich Office- und SharePoint-Produkten. Die Organisation liefert Inhalte und Dokumente, die von Microsoft in das erforderliche Format für das Dokumentenmanagement umgewandelt und auf den entsprechenden Plattformen bereitgestellt werden.

- *Citrix in den Bereichen ADC und Virtualisierung*: Citrix stellt die Infrastruktur und Software für Application Delivery Control und Virtualisierungslösungen zur Verfügung. Die Organisation nutzt diese Dienste, um ihre Anwendungen und Netzwerke zu managen, wobei Citrix die erforderlichen Werkzeuge und Support für die Virtualisierung und Netzwerksicherheit bereitstellt.
- *Evacon für das Digitale Kirchenbuch (DKB)*: Die evacon IT-Solution & Consulting GmbH & Co. KG koordiniert die Entwicklung der Anwendung für das Digitale Kirchenbuch.
- *KRZ-SWD*: Die Stiftung Kirchliches Rechenzentrum Südwestdeutschland ist verantwortlich für die Wartung, Entwicklung und den Betrieb des kirchlichen Meldewesens
- *ECKD für KFM*: Die ECKD GmbH ist verantwortlich für die Bereitstellung und Wartung der KFM-Software. Die Organisation liefert Finanzdaten, die von ECKD in das KFM-System integriert und für Finanzverwaltungszwecke verwendet werden.
- *Oberkirchenrat Württemberg für PersonalOffice*: *Oberkirchenrat* Württemberg bietet Hosting für die PersonalOffice-Software.
- Scopevisio für Phoenix: Die Scopevisio Content Solutions GmbH stellt die Phoenix-Software zur Verfügung und ist für deren Wartung zuständig.
- *CT Systeme (Falk) / SF Software-Beratung für SF Buchungsplan und SF Kirchensteuerkappung*: Dieser Dienstleister ist zuständig für die Bereitstellung und Wartung der entsprechenden Finanzsoftware.
- *TelemaxX für Netzwerk und Infrastruktur*: Die TelemaxX Telekommunikation GmbH ist verantwortlich für das Hosting und die Wartung der Netzwerkinfrastruktur im Rechenzentrum. Die Organisation nutzt diese Infrastruktur für ihre IT-Systeme, wobei TelemaxX die erforderlichen Dienste für Netzwerksicherheit und -performance bereitstellt.

4 IT-STRUKTURANALYSE

4.1 Bereinigter Netzplan

Siehe Anhang „bereinigter Netzplan“.

4.2 Wesentliche IT-Anwendungen und IT-Systeme

Für den Zugriff auf dieses Dokument und weitere Informationen zu unserer Sicherheitspolitik und -praktiken, verweisen wir auf den entsprechenden Abschnitt insbesondere „Schutzbedarf-Produkte“ im ISMS.

4.3 Netzwerkstruktur und räumliche Gegebenheiten

Für den Zugriff auf Informationen zu unserer Sicherheitspolitik und -praktiken, verweisen wir auf den entsprechenden Abschnitt insbesondere „Gebäudeplan Schutzkonzept“ im ISMS sowie unsere Dokumentation in i-Do-It.

5 SCHUTZBEDARFSFESTSTELLUNG

5.1 Erhebung des Schutzbedarfs für IT-Anwendungen

Für den Zugriff auf dieses Dokument und weitere Informationen zu unserer Sicherheitspolitik und -praktiken, verweisen wir auf den entsprechenden Abschnitt insbesondere „Schutzbedarf-Produkte“ im ISMS.

5.2 IT-Systeme

Für den Zugriff auf dieses Dokument und weitere Informationen zu unserer Sicherheitspolitik und -praktiken, verweisen wir auf den entsprechenden Abschnitt insbesondere „Schutzbedarf-Produkte“ im ISMS.

5.3 Netze/Kommunikationsverbindungen

Es liegt eine direkte Leitung zum Rechenzentrum von TelemaxX in Karlsruhe. Danach finden die Redundanzen und Sicherheitsmaßnahmen des Rechenzentrums Anwendung.

5.4 Räume und Gebäude

Die detaillierte Dokumentation der räumlichen Gegebenheiten und der Hardware wird in unserem zentralen IT-Dokumentationssystem i-doit geführt. Dort sind folgende Informationen hinterlegt:

- Gebäudestruktur und Raumaufteilung
- Zutrittskontrollsysteme und deren Verwaltung
- Standorte kritischer IT-Infrastruktur (z.B. Serverräume, Netzwerkverteiler)
- Physische Sicherheitsmaßnahmen (z.B. Überwachungskameras, Alarmsysteme)

Für eine detaillierte Einsicht in die spezifischen Schutzmaßnahmen und Sicherheitskonzepte der einzelnen Räumlichkeiten verweisen wir auf die entsprechenden Einträge in i-doit. Die Zugriffsrechte auf diese sensiblen Informationen sind streng reguliert und werden nur autorisierten Personen gewährt.

Die regelmäßige Überprüfung und Aktualisierung dieser Informationen in i-doit ist Teil unseres kontinuierlichen Verbesserungsprozesses im Rahmen des Informationssicherheitsmanagements.

6 ISMS und STATEMENT OF APPLICABILITY

Im Rahmen der Implementierung und Aufrechterhaltung unseres Informationssicherheits-Managementsystems (ISMS) wurde das System gemäß den Standards der ISO27001:2022 und ISO27002:2022 konzipiert und entwickelt. Diese international anerkannten Standards bilden die Grundlage für eine umfassende und effektive Sicherheitsstrategie, die darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit unserer Informationen zu schützen und zu gewährleisten.

Für die Einhaltung dieser Normen wurden spezifische Dokumente erstellt und im ISMS hinterlegt. Diese Dokumentation ist ein entscheidender Bestandteil unseres Sicherheitsframeworks und

beinhaltet Richtlinien, Verfahren und Kontrollen, die speziell darauf ausgerichtet sind, die Sicherheitsanforderungen der ISO27001:2022 und ISO27002:2022 zu erfüllen.

Ein zentrales Element innerhalb dieser Dokumentation ist das "Statement of Applicability". Dieses Dokument ist von entscheidender Bedeutung, da es eine detaillierte Übersicht über die Anwendbarkeit der verschiedenen Sicherheitskontrollen bietet, die im Rahmen der ISO-Normen identifiziert wurden. Es beschreibt, welche Kontrollen implementiert wurden, und liefert Begründungen für die Aufnahme oder den Ausschluss spezifischer Kontrollen im Kontext unserer Organisation.

Das "Statement of Applicability" ist ein dynamisches Dokument, das regelmäßig überprüft und aktualisiert wird, um sicherzustellen, dass es weiterhin die aktuellen Sicherheitsanforderungen und organisatorischen Veränderungen widerspiegelt. Es dient nicht nur als Nachweis für die Einhaltung der ISO-Standards, sondern auch als Leitfaden für die kontinuierliche Verbesserung unseres ISMS.

Das vollständige "Statement of Applicability" kann im ISMS eingesehen werden. Für den Zugriff auf dieses Dokument und weitere Informationen zu unserer Sicherheitspolitik und -praktiken, verweisen wir auf den entsprechenden Abschnitt im ISMS.

7 BASIS-SICHERHEITSCHECK

Für den Zugriff auf dieses Dokument und weitere Informationen zu unserer Sicherheitspolitik und -praktiken, verweisen wir auf den entsprechenden Abschnitt im ISMS.

8 Gefährdungsanalyse

Die „Gefährdungsanalyse“ ist ebenfalls im ISMS zu finden.

9 Inkraftsetzung

Das Sicherheitskonzept ist bei jeder Änderung der aktuellen örtlichen und personellen Gegebenheiten und aus sonstigen Anlässen, die Auswirkungen auf das Sicherheitskonzept haben, fortzuschreiben und spätestens nach einem Jahr zu überprüfen.

Das Sicherheitskonzept mit Wirkung zum 1. Juli 2017 in Kraft. Die aktuelle vorliegende überarbeitete Version wird zum 15.02.2024 in Kraft gesetzt.

Karlsruhe	13.02.2024
Ort	Datum
Uta Henke	Alfred Ernst
Geschäftsleitende Oberkirchenrätin	ISB / DSB