Evangelische Landeskirche in Baden
Evangelischer Oberkirchenrat

EVANGELISCHE LANDESKIRCHE IN BADEN

Informationssicherheitsleitlinie

INHALTSVERZEICHNIS

1 Dokumenteninformation

1.1 Dokumentendaten

Typ	Dokumenten Verantwortlicher	Version
Leitlinie	Informationssicherheitsbeauftragter (ISB)	Siehe Info im SharePoint

1.2 Dokumentenhistorie

Letzte Änderung	Bearbeiter	Status	Freigabe am	Freigabe durch
2023-10-18	Yannick Lackus	In Arbeit	19.02.2024	Frau Henke

1.3 Beteiligte Personen

Name	E-Mail-Adresse	Telefonnummer	Rolle
Robin Leitner	Robin.leitner@secudor.de		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

1.4 Mitgeltende Dokumente

Keine mitgeltenden Dokumente

1.5 Rechtliche Grundlage

Für die Handhabung und den Schutz von Informationen des Evangelischen Oberkirchenrats Karlsruhe (EOK) orientiert sich dieser an dem internationalen Standard ISO/IEC 27001:2022, welcher die Anforderungen für Informationssicherheits-Managementsysteme (ISMS) festlegt. Dies stellt eine gezielte Entscheidung des EOK 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 der EOK für die Anwendung der ISO/IEC 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 Allgemein

2.1 Zweck des Dokuments

Die vielfältigen Aufgaben des Evangelischen Oberkirchenrats Karlsruhe (EOK) sind in wachsendem Umfang auf Informations- und Kommunikationstechnologien angewiesen. Solche Technologien eröffnen sowohl Möglichkeiten, die wir nutzen wollen, als auch Risiken, denen wir angemessen begegnen müssen.

Jede Information innerhalb des EOK repräsentiert einen Wert und verdient daher entsprechenden Schutz. Der Schutz von Informationen und die Sicherheit der IT-Systeme sind daher eine wichtige Aufgabe für die Verantwortlichen, um die Integrität unserer kirchlichen Arbeit zu gewährleisten und das geistige Eigentum des EOK zu schützen.

Daher ist es für den EOK unerlässlich, eine Leitlinie für die Informationssicherheit zu etablieren, die für alle Abteilungen und Organisationseinheiten innerhalb des EOK verbindlich ist.

2.2 Bedeutung der Informationssicherheit

Der EOK ist von der zeitnahen Verarbeitung elektronischer und nichtelektronischer Informationen abhängig. Von größter Wichtigkeit ist neben der Verfügbarkeit und der Integrität auch die Vertraulichkeit der Informationen. Jeder Mitarbeitende muss sich daher der Notwendigkeit der Informationssicherheit und des Informationsschutzes bewusst sein und entsprechend handeln. Diese Maßnahmen sind nicht nur gesetzlich vorgeschrieben, sondern auch Teil der Verpflichtungen der EKIBA gegenüber Aufsichtsbehörden und besonders den Kunden.

2.3 Geltungsbereich der Leitlinie zur Informationssicherheit

Diese Leitlinie zur Informationssicherheit gilt verbindlich für alle Organisationseinheiten innerhalb des EOK, der EH-Freiburg und soweit anwendbar für externe Mitarbeitende. Diese Leitlinie wird durch Sicherheitsrichtlinien etc. ausgestaltet.

3 Verpflichtung jedes einzelnen Mitarbeitenden

Diese Leitlinie zur Informationssicherheit ist für alle Mitarbeitenden des EOK und der EH-Freiburg verpflichtend. Alle Mitarbeitenden sind aufgefordert, aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden teilzunehmen, umsichtig mit den Informationssystemen und den darauf gespeicherten und verarbeiteten Daten umzugehen und bei Unregelmäßigkeiten den Informationssicherheitsbeauftragten umgehend zu informieren.

4 Prinzipien der Informationssicherheit

Für den EOK gelten folgende Sicherheitsprinzipien:

4.1 Sicherheit im Vordergrund (Nützlichkeitserwägung)

Um die Sicherheit von Informationen und Informationstechnik zu gewährleisten und Schäden abzuwehren, müssen mögliche Einschränkungen im Komfort von IT-Systemen akzeptiert werden.

4.2 Minimalprinzip

Der Zugriff auf und der Zugang zu sicherheitskritischen IT-Systeme, IT-Anwendungen und Informationen, wird auf einen minimalen Personenkreis eingeschränkt.

4.3 Need-to-Know-Prinzip

Jeder Mitarbeitende erhält Zugriff ausschließlich auf diejenigen IT-Anwendungen und Informationen, die zur Erfüllung der jeweiligen Aufgabe erforderlich sind. Dabei ist immer gegen den Schutzbedarf der jeweiligen IT-Systeme, IT-Anwendungen und Informationen gemäß Minimalprinzip abzuwägen.

5 Sicherheitsziele

Für den EOK gelten folgende Sicherheitsziele:

- Gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen müssen erfüllt werden. Insbesondere sind auch einschlägige Gesetze der Länder, in denen sich Organisationseinheiten befinden, einzuhalten
- Die Vertraulichkeit muss gewährleistet werden. D.h. dass keine unberechtigte Person Daten des EOK einsehen darf
- Die Integrität muss sichergestellt werden. D.h. dass keine Veränderungen an Daten von Unbefugten stattfinden dürfen. Weiterhin dürfen keine Daten ohne Protokoll verändert werden.
- Die Verfügbarkeit muss sichergestellt werden. D.h. dass keine Daten ungewollt gelöscht oder nicht nutzbar werden.

6 Sicherheitsprozess

Der EOK setzt einen Sicherheitsprozess in Gang, der sich an dem ISO/IEC 27001 Standard beschriebenen Plan-Do-Check-Act (PDCA) Kontrollprozess orientiert.

Bei der Etablierung des Sicherheitsprozesses verpflichtet sich der EOK zur Einhaltung folgender Rahmenbedingungen:

1. Der Sicherheitsprozess wird durch die Verabschiedung einer Leitlinie zur Informationssicherheit initiiert
2. Es gilt ein einheitliches Berichtswesen
3. Nachvollziehbare Dokumentation des Vorgehens und der Bewertungskategorien bei der Risikoanalyse ebenso wie eine einheitliche Datenklassifikation
4. Durchführung regelmäßiger Audits gemäß Richtlinie

7 Informationssicherheits-Team

7.1 Beschreibung des Teams

Das Informationssicherheitsteam setzt sich aus dem Informationssicherheitsbeauftragten (ISB), dem Datenschutzbeauftragten, dem IT-Leiter und der Geschäftsleitung zusammen.

7.2 Aufgaben und Verantwortlichkeiten

Dieses Team ist verantwortlich für die Gesamtkoordination der Informationssicherheit innerhalb der Organisation. Es trifft Entscheidungen zu Richtlinien, überwacht die Implementierung von Sicherheitsmaßnahmen und bewertet regelmäßig die Effektivität der Informationssicherheitsstrategie.

7.3 Kommunikation und Berichterstattung

Das Team stellt sicher, dass alle relevanten Sicherheitsinformationen effektiv kommuniziert werden und berichtet regelmäßig an die Geschäftsleitung und andere Stakeholder über den Status der Informationssicherheit.

7.4 Notfall- und Krisenmanagement

Das Team spielt eine zentrale Rolle im Management von Sicherheitsvorfällen und Krisensituationen, indem es schnelle und effektive Maßnahmen zur Eindämmung und Behebung von Sicherheitsvorfällen ergreift.

8 Sicherheitsrichtlinien

Sicherheitsrichtlinien dienen der thematischen Regelung und Steuerung mithilfe von Maßnahmen. Diese Sicherheitsrichtlinien werden im Rahmen des Sicherheitsprozesses angepasst, ergänzt oder außer Kraft gesetzt. Die Sicherheitsrichtlinien sind für alle Mitarbeitenden frei zugänglich und einsehbar zur Verfügung zu stellen.

9 Sicherheitsorganisation

9.1 Organisatorische Sicherheitsstruktur

Eine tragfähige Informationssicherheit ist nur in Teamarbeit unter aktiver Mitarbeit jedes einzelnen Mitarbeitenden möglich.

Dazu ist es erforderlich, konkrete technische und organisatorische Schutzziele zu definieren und umzusetzen, angepasst an die Belange der einzelnen IT-Systeme, IT-Anwendungen und Informationen. Um dies zu erreichen, ist eine Sicherheitsorganisation gemäß dem beiliegenden Organigramm etabliert.

Die Geschäftsleitung des EOK ist für die Informationssicherheit der internen Abteilungen verantwortlich und verabschiedet die vorliegende Sicherheitsleitlinie. Eine Rollenbeschreibung ist aus dem Dokument „Rollenbeschreibung“ zu entnehmen.

9.2 Externe Mitarbeitende

Lieferanten (unter Umständen der einzelne externe Mitarbeitende) sind durch interne Mitarbeitende über die einschlägigen Richtlinien und Handlungsanweisungen in der Kirche zu informieren. Das Einverständnis zur Befolgung der Schutzmaßnahmen zur Informationssicherheit ist schriftlich einzuholen. Eine Verweigerung des Einverständnisses eines Lieferanten führt zu einer Beendigung der Geschäftsbeziehung, wenn nicht andere Gründe dagegensprechen.

10 Durchsetzung

Die Durchsetzung dieser Rahmenregelung wird für den EOK durch die Geschäftsleitung des Evangelischen Oberkirchenrats Karlsruhe geregelt. Bestandteil dieser Regelung ist die hier vorliegende Leitlinie zur Informationssicherheit sowie die dazugehörigen Informationssicherheitsrichtlinien.

11 Sicherheitsdokumentation

Die nachfolgende Übersicht bietet eine strukturierte Darstellung der verschiedenen Bereiche und Aspekte, die im Rahmen eines umfassenden Informationssicherheits-Managementsystems berücksichtigt werden sollten:

00_Organisation

Dieser Bereich beschäftigt sich mit der strukturellen und organisatorischen Einrichtung der Informationssicherheit. Er beinhaltet Aspekte wie Verantwortlichkeiten, Aufgabenverteilung und die interne Organisationsstruktur.

01_Leitlinien

Hier sind die grundlegenden Prinzipien und Werte festgelegt, die die Basis für sämtliche sicherheitsrelevanten Maßnahmen und Entscheidungen bilden.

02_Verzeichnisse

In diesem Abschnitt werden alle wichtigen Verzeichnisse geführt, z. B. über Assets, Verarbeitungsaktivitäten oder Risiken.

03_Richtlinien

Dieser Bereich enthält konkrete Anweisungen und Vorgaben, wie bestimmte sicherheitsrelevante Prozesse und Tätigkeiten durchgeführt werden sollen.

04_Information

Hier werden Informationen zentral bereitgestellt, beispielsweise Updates zu Sicherheitsvorfällen, Neuerungen im Sicherheitsmanagement oder allgemeine Kommunikationen.

05_Awareness

Dieser Abschnitt befasst sich mit der Sensibilisierung und Schulung von Mitarbeitern. Ziel ist es, das Bewusstsein für Sicherheitsrisiken zu erhöhen und präventives Verhalten zu fördern.

06_Verträge_Vereinbarungen

In diesem Bereich werden alle vertraglichen Regelungen und Vereinbarungen erfasst, die einen Bezug zur Informationssicherheit haben, etwa Dienstleisterverträge oder Geheimhaltungsvereinbarungen.

07_Dokumentationen

Hier werden alle Formen von Dokumentationen bezüglich der Informationssicherheit gesammelt, wie Vorfalls-Meldungen (wenn nicht bereits woanders dokumentiert), Handbücher oder Protokolle.

08_Audits

In diesem Abschnitt geht es um die regelmäßige Überprüfung und Bewertung der Informationssicherheitsmaßnahmen. Audits helfen dabei, die Effektivität von Prozessen zu bewerten und potenzielle Schwachstellen zu identifizieren.

99_Sonstiges

Dieser Bereich dient als Sammelstelle für alle weiteren Dokumente und Informationen, die nicht in die vorherigen Kategorien fallen, aber dennoch für das Thema Informationssicherheit relevant sind.