**LS 2014 Drucksache 22**

**Vorlage der Kirchenleitung an die Landessynode**

# Informationstechnologie

## A

## BESCHLUSSANTRAG

1. Die in Erledigung des Beschlusses 55 der Landessynode 2013 vorgelegten Arbeitsergebnisse werden mit Dank entgegen genommen.

2. Die Beschlussfassung über ein Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland wird bis zur Landessynode 2015 ausgesetzt. Im Zuge der weiteren Beratungen soll insbesondere diskutiert werden, ob die Einheitlichkeit dadurch hinreichend gewährleistet ist, dass gesetzlich empfohlen wird, dass die Kreissynode für den Kirchenkreis, seine Werke und Einrichtungen und die ihm angehörenden Kirchengemeinden ein einheitliches IT-Konzept beschließt.

3. Die Kirchenleitung wird beauftragt, in der ersten Hälfte des Jahres 2014 in regionalen Fachkonferenzen die Notwendigkeit und den Regelungsgehalt des IT-Rahmenkonzeptes zu vermitteln und hierbei insbesondere die Aspekte Wirtschaftlichkeit, IT-Sicherheit und Verbindlichkeit zu thematisieren. Der von der Kirchenleitung mit Beschluss vom 19.04.2013 berufene Lenkungsausschuss soll die regionalen Fachkonferenzen vorbereiten und an der Erstellung des IT-Rahmenkonzepts beteiligt werden.

4. Die Kirchenleitung wird beauftragt, das IT-Rahmenkonzept zu erstellen. Für die Erstellung des IT-Rahmenkonzeptes und die Tätigkeit des IT-Lenkungsausschusses sowie die Durchführung der regionalen Fachkonferenzen werden 210.000,00 Euro bereitgestellt. Die Finanzierung erfolgt entsprechend dem Anteil der Kirchengemeinden und dem Anteil der Landeskirche am Kirchensteueraufkommen (89,9%/10.1%).

**B**

**BEGRÜNDUNG**

## Übersicht

## 1. Landessynodale Beschlusslage zum Thema Informationstechnologie (IT)

Mit Beschluss Nr. 55 **(Anlage 1)** hat die Landessynode 2013 die Kirchenleitung beauftragt, der Landessynode 2014 einen Beschlussantrag zu unterbreiten, wie die mit Beschluss Nr. 75 (**Anlage 2)** der Landessynode 2012 angestrebte Vereinheitlichung der Informationstechnologie in der Evangelischen Kirche im Rheinland verwirklicht werden soll. Der Auftrag beinhaltet insbesondere die Definition verbindlicher IT-Standards zur Wahrung von Informationssicherheit und Datenschutz. Weiterhin soll ein struktureller und rechtlicher Rahmen für den Vollzug des operativen Betriebs zur Entscheidung vorgeschlagen werden, der Nachhaltigkeit sichert.
Zur Begleitung und Überwachung der Erledigung des Arbeitsauftrages ist die Berufung eines Lenkungsausschusses vorgesehen, der der Kirchenleitung die Ergebnisse vorlegt.

## 2. Zusammensetzung und Arbeitsweise des Lenkungsausschusses

Die Zusammensetzung des Lenkungsausschusses geht aus **Anlage 3** hervor.
Der Lenkungsausschuss wurde durch das Landeskirchenamt, insbesondere den Bereich des Vizepräsidenten und das Dezernat V.1 (Recht), unterstützt. Außerdem berief der Lenkungsausschuss eine Projektgruppe, bestehend aus kirchlichen Kompetenzträgern, d.h. IT-Verantwortlichen aus Kirchenkreisen. Die Projektgruppe wurde durch eine externe Begleitung unterstützt, namentlich durch die Fa. HiSolutions. Kernaufgabe der Projektgruppe war die Definition von IT-Anforderungen, darüber hinaus hat sich die Projektgruppe auf Wunsch des Lenkungsausschusses auch mit der Organisationsfrage befasst.
Die Arbeit der Projektgruppe wurde dadurch erschwert, dass es zum einen nur wenige IT-Fachleute gibt, die überwiegend mit anspruchsvollen IT-Aufgaben betraut sind. Zum anderen waren Mitglieder der Projektgruppe aus verschiedenen Gründen an einer kontinuierlichen Mitarbeit gehindert. Die Projektgruppe konnte dennoch ihre wesentlichen Aufgaben erfüllen. Es fanden insgesamt 10 Sitzungen der Projektgruppe statt.
Der Lenkungsausschuss hat sich im Hinblick auf die Organisationsfrage der Unterstützung der Fa. Kienbaum bedient, die im Zuge der Verwaltungsstrukturreform berät. Auf diese Weise wurde auch die Verbindung zu diesem Vorhaben in die Betrachtungen mit einbezogen.
Der Lenkungsausschuss traf sich zu sieben Sitzungen.
Die Datenschutzbeauftragte wurde jeweils mit eingeladen. Zwei Mitglieder der Projektgruppe nahmen zwecks Berichterstattung an den Sitzungen der Lenkungsgruppe teil.

## 3. Ergebnis der Beratungen des Lenkungsausschusses

Der Lenkungsausschuss ist zu dem Ergebnis gekommen, dass ein Kirchengesetz.über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland erlassen werden soll, um die mit dem Auftrag der Landessynode verfolgten Ziele zu erreichen..
Ein entsprechender Gesetzentwurf wurde durch das Landeskirchenamt erarbeitet. Nachfolgend werden der Gesetzentwurf und seine Begründung (3.1 und 3.2) sowie – als wesentlicher Regelungsbestandteil - die Struktur eines IT-Rahmenkonzeptes (3.3) wiedergegeben.

Des Weiteren wird das alternative Modell einer landeskirchenweiten Organisation, das der IT-Lenkungsausschuss beschrieben, jedoch nicht zur Umsetzung vorgeschlagen hat, entfaltet (3.4).

### 3.1 Entwurf eines Kirchengesetzes über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland:

**Kirchengesetz über den Einsatz**
**von Informations- und Kommunikationstechnik**
**in der Evangelischen Kirche im Rheinland**
**(– ITG –)**
**Vom**
(KABl.)

**Inhaltsübersicht***



***Die Inhaltsübersicht ist nicht Bestandteil dieses Gesetzes.

## § 1
## Anwendungsbereich

(1) Dieses Gesetz regelt die Anwendung und den Gebrauch von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland.

(2) Die der Evangelischen Kirche im Rheinland zugeordneten rechtlich eigenständigen Einrichtungen können dieses Gesetz ganz oder in Teilen für anwendbar erklären.

(3) Die Regelungen des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG.EKD), der Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung - ITSVO-EKD) und des Mitarbeitervertretungsgesetzes (MVG - EKiR) bleiben unberührt.

## § 2
## Grundsätze

(1) Der Einsatz von Informationstechnik (IT) unterstützt die Erfüllung des kirchlichen Auftrags.

(2) $_1$Informationstechnik (IT) hat die Sicherheit der automatisierten Verarbeitung von Daten zu gewährleisten. $_2$Sie soll im Interesse der Anwenderinnen und Anwender gebrauchstauglich sein.

(3) Einheitliche Informations- und Kommunikationstechnik wird zur Verbesserung der Zusammenarbeit, der Gewährleistung eines einheitlichen Sicherheitsstandards, der Wirtschaftlichkeit und Nachhaltigkeit auf allen Ebenen der Evangelischen Kirche im Rheinland entwickelt und eingesetzt.

## § 3
## Begriffsbestimmungen

(1) Informationstechnik (IT) im Sinne dieses Gesetzes umfasst alle technischen Mittel zur automatisierten Verarbeitung von Daten.

(2) Kommunikationstechnik (KT) ist die Informationstechnik, die von einer oder mehreren kirchlichen Einrichtungen oder im Auftrag einer oder mehrerer kirchlicher Einrichtungen betrieben wird und die der Kommunikation oder dem Datenaustausch untereinander oder mit Dritten dient.

(3) Sicherheitsrisiken sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion informationstechnischer Systeme beeinflussen können.

## § 4
## IT - Rahmenkonzept

(1) $_1$Die Kirchenleitung fördert die Sicherheit in der Informations- und Kommunikationstechnik sowie die Nachhaltigkeit bei einheitlichen informationstechnischen Lösungen. $_2$Hierzu beschließt sie ein regelmäßig fortzuschreibendes „Rahmenkonzept zur Informations- und Kommunikationstechnologie der Evangelischen Kirche im Rheinland (IT-Rahmenkonzept)“. $_3$ Die Kirchenleitung erlässt das IT-Rahmenkonzept der Evangelischen Kirche im Rheinland als Verordnung, mit der die Anforderungen an die kirchengesetzlichen Vorschriften zum Datenschutz und der IT-Sicherheit erfüllt sind.

(2) $_1$Das IT-Rahmenkonzept im Sinne dieses Gesetzes beinhaltet die umfassende Zusammenstellung der Ziele und daraus abgeleiteten Strategien und Maßnahmen zur Umsetzung der Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland. $_2$Das Rahmenkonzept hat die dazu notwendigen Informationen und Begründungszusammenhänge, eine Chancen-Risiken-Abwägung sowie einen Zeit- und Maßnahmenplan und eine Ressourcenplanung (Zeit, Geld, Material, Personal) zu enthalten. $_3$Es hat die Anforderungen von § 9 Abs. 2 DSG.EKD zu erfüllen.

(3) Die Kirchenleitung beschließt entsprechend der technischen und rechtlichen Anforderungen des IT-Rahmenkonzeptes einzelne Verfahren als verbindliche Referenzlösungen, wenn ein gesamtkirchliches Interesse besteht.

## § 5
## IT-Kommission

(1) $_1$Die Kirchenleitung beruft zu ihrer Unterstützung bei der Erstellung und der Fortschreibung des IT-Rahmenkonzeptes eine ständige IT-Kommission, die aus höchstens zehn Mitgliedern besteht. Die Berufung soll sich an fachlichen Gesichtspunkten orientieren. $_2$Die Geschäftsführung wird durch das Landeskirchenamt erledigt.

(2) Die Kommission gibt sich eine Geschäftsordnung.

(3) Die Kommission hat insbesondere folgende Aufgaben:

a) Abwehr von Gefahren für die Sicherheit der Informationstechnik;

b) Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, soweit dies zur Erfüllung der Aufgaben erforderlich ist;

c) Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen und Komponenten sowie Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;

d) Prüfung, Bewertung und Einführung einheitlicher informations- und kommunikationstechnischer Systeme für alle Ebenen der Evangelischen Kirche im Rheinland;

e) Sicherung der Datenqualität bei einheitlichen Lösungen;

f) Sicherstellung des laufenden Betriebes bei einheitlichen Lösungen und

g) Erarbeitung von Vorschlägen an die Kirchenleitung für Referenzlösungen.

## § 6
## IT – Finanzkommission

(1) Die Kirchenleitung beruft eine von der IT-Kommission unabhängigen, aus 3 Personen bestehende IT – Finanzkommission.

(2) Die Aufgabe der IT – Finanzkommission besteht darin, die Entwicklung der Kosten und Aufwände der IT-Anwendungen und -Lösungen, die sich aus dem IT-Rahmenkonzept ergeben, zu analysieren und zu prüfen. Dazu hat sie ständig zu kontrollieren, welche Kosten- und Aufwandsentwicklungen sich aus der fortlaufenden Weiterentwicklung des IT-Rahmenkonzeptes sowie im Hinblick auf die Anpassung von bestehenden IT-Lösungen zukünftig ergeben.

(3) Vor der Entscheidung durch die Kirchenleitung für eine Referenzlösung gemäß § 4 Absatz 2 hat die IT – Finanzkommission im Vorfeld der Vergabe auch Kosten- und Aufwandsentwicklung von Vergleichsangeboten zu überprüfen und eine entsprechende Empfehlung an die Kirchenleitung abzugeben.

(4) In die Analysen und Prüfungen gemäß der Absätze 2 und 3 sind insbesondere auch Folgekosten, die durch Beratungs-, Schulungs- und Anpassungsbedarf entstehen, mit einzubeziehen.

(5) Unbeschadet der Zuständigkeit des Finanzausschusses hat sie ihre Prüfergebnisse der Kirchenleitung unabhängig von der IT-Kommission anlassbezogen, wenigstens aber jährlich zur Entscheidung vorzulegen.

## § 7
## Einheitlichkeit

(1) Alle kirchlichen Körperschaften haben ein IT-Konzept nach Maßgabe von § 4 Absatz 3 zu erstellen. Es wird empfohlen, dass die Kreissynode für den Kirchenkreis, seine Werke und Einrichtungen und die ihm angehörenden Kirchengemeinden ein einheitliches IT-Konzept beschließt.

(2) Das IT Rahmenkonzept der Evangelischen Kirche im Rheinland gilt für kirchliche Körperschaften als IT Konzept, wenn sie die dem IT-Rahmenkonzept entsprechenden Lösungen und Anwendungen einsetzen.

(3) Die Kosten, die den kirchlichen Körperschaften durch den Einsatz von Informations- und Kommunikationstechnik Lösungen entstehen, die den beschlossenen Referenzlösungen entsprechen, werden gesamtkirchlich getragen, soweit sie den im IT-Rahmenkonzept vorgesehenen verpflichtenden Anforderungen entsprechen.

(4) Soweit kirchliche Körperschaften der Evangelischen Kirche im Rheinland eigene, nicht der Rahmenkonzeption im Sinne von § 4 Absatz 1 Satz 2 entsprechende eigenen Lösungen im Bereich der Informations- und Kommunikationstechnik einsetzen und anwenden, haben sie die dadurch entstehenden Kosten und Aufwände selbst zu tragen.

## § 8
## Beteiligung

(1) Bei der Erstellung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl von Programmen, über die personenbezogene Daten verwaltet werden, ist die oder der Betriebsbeauftragte oder die oder der örtlich Beauftragte für den Datenschutz frühzeitig zu beteiligen.

(2) Die Beteiligung der Mitarbeitervertretung entsprechend dem Mitarbeitervertretungsgesetz (MVG - EKiR) in der jeweils geltenden Fassung ist zu gewährleisten.

**§ 9**
**Datenverarbeitung im Auftrag**

$_1$Die Vorschriften des Kirchengesetzes über den Datenschutz der Evangelischen Kirche In Deutschland für die Datenverarbeitung im Auftrag finden entsprechend Anwendung. $_2$Vor einer Beauftragung ist die Genehmigung des Landeskirchenamtes einzuholen.

**§ 10**
**Durchführungsbestimmungen**

Die Kirchenleitung kann Durchführungsbestimmungen zu diesem Gesetz erlassen.

**§ 11**
**Inkrafttreten**

(1) Dieses Gesetz tritt am in Kraft.

(2) Dieses Gesetz soll spätestens nach Ablauf von 5 Jahren nach dem Inkrafttreten von der Landessynode überprüft werden.

## 3.2 Begründung des Gesetzentwurfes

Im Verlauf der letzten Jahre hat sich die Informations- und Kommunikationstechnologie zu einer der zentralen Säulen für die Leistungsfähigkeit moderner kirchlicher Strukturen innerhalb und außerhalb ihrer verfassten Organe entfaltet. Da die IT-Entwicklung innerhalb der Evangelischen Kirche im Rheinland zum Teil sehr unkoordiniert verlaufen ist, hat die Landessynode 2013 den Auftrag erteilt, zu prüfen, wie die von der Landessynode 2012 angestrebte Vereinheitlichung der Anwendung von Informationstechnologie in der Evangelischen Kirche im Rheinland verwirklicht werden kann.

Der Einsatz von Informations- und Kommunikationstechnik hat sich in den vergangenen Jahren zu einem der wichtigsten Arbeitsmittel für die Abläufe kirchlicher Verwaltung und Kommunikation entwickelt. Daraus resultiert ein

hoher Anspruch an die Betriebsstabilität und Verfügbarkeit der IT-Systeme. Ziel ist es, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten in Zukunft sicherzustellen. Hierfür müssen organisatorische Maßnahmen ergriffen werden, die durch funktionale und technisch- infrastrukturelle Komponenten zu ergänzen sind. Darüber hinaus soll durch Abstimmung und weitgehende Koordinierung ein möglichst hohes Maß an Synergieeffekten erzielt werden.

Grundsätzlich sind bei allen Organisationsstrukturen, gleichgültig ob im Bereich des Privatrechtes oder des öffentlichen Rechtes, die jeweils gesetzliche bestimmten Leitungsorgane rechtlich verantwortlich für die Einhaltung des Datenschutzes und der IT Sicherheit. Dies gilt auch für die kirchlichen Leitungsorgane.

Die komplexen und größtenteils technisch orientierten Anforderungen können nicht in einem gesetzlichen Regelungswerk dargestellt werden. Deshalb ist es in allen großen rechtlich und wirtschaftlich zusammenhängenden Systemen üblich und erforderlich, sogenannte IT Rahmenkonzepte zu entwickeln, mit denen diese Anforderungen beschrieben, identifiziert und letztlich technischen Lösungen zugeführt werden, um das Haftungsrisiko der Leitungsorgane zu minimieren.

Das Kirchengesetz soll

- zum ersten die Verpflichtung zur Erstellung eines IT Rahmenkonzeptes an die Leitungsorgane der Evangelischen Kirche im Rheinland adressieren,

- zum zweiten die Anforderungen des Datenschutzgesetzes der EKD, insbesondere die der Anforderungen an die IT- Sicherheit, durch das Angebot der Übernahme eines IT-Rahmenkonzeptes regeln und damit das Haftungsrisiko der Leitungsorgane auf ein Mindestmaß begrenzen, und

- zum dritten die Entscheidungsoptionen für abweichende IT Lösungen und Anwendungen in eigener Verantwortung eröffnen.

Der Gesetzesentwurf berücksichtigt die historisch gewachsene Struktur der Evangelischen Kirche im Rheinland im Hinblick auf die Selbstständigkeit und Autonomie kirchlicher Körperschaften. Diese Betrachtungsweise ist für die von der Landessynode geforderte Einheitlichkeit des Einsatzes von IT grundlegend, weil sich der Einsatz und die Anwendung von Informations- und Kommunikationstechnologie in den kirchlichen Körperschaften Hand in Hand mit inhaltlichen Schwerpunktsetzungen und der ständigen

Veränderung kirchlicher Arbeit entwickelt hat; IT also gewissermaßen das Spiegelbild kirchlicher Arbeit darstellt.

Vor diesem Hintergrund regelt der Gesetzesentwurf zunächst entsprechend den Vorschriften des Datenschutzgesetzes der EKD die generelle Zuständigkeit der Kirchenleitung als verantwortliches Leitungsorgan zur Erstellung eines IT-Rahmenkonzeptes.

Das IT Rahmenkonzept i.S.v. § 4 Abs. 2 beschreibt beginnend mit dem ersten Einsatz von elektronischer Datenverarbeitung die gesamte IT Entwicklung in der Evangelischen Kirche im Rheinland. Dabei ist die Beschreibung nicht nur auf die landeskirchliche Ebene beschränkt, sondern hat auch, jedenfalls in der Tendenz, die Entwicklung der Kirchenkreise und Gemeinden zu analysieren und zu beachten. Eine derartige Analyse und Evaluierung ist deshalb erforderlich, weil nur so das eigene Verständnis aktiviert werden kann, warum in der Landeskirche gegenwärtige Lösungen eingesetzt und zukünftige Lösungen angestrebt werden.

Das IT Rahmenkonzept i. S. d. Gesetzes umfasst die Beschreibung aller sicherheitsrelevanten Bereiche, weist Berechtigungsstrukturen und deren Regelungen auf und bietet Muster für Verpflichtungserklärungen an, die für einzelne Mitarbeitende gelten, die entweder mit besonders empfindlichen Daten, in gefährdeten Bereichen oder mit Systemen arbeiten, die nicht vom IT Konzept erfasst sind. Hierunter fällt zum Beispiel der dienstliche Einsatz privater Handys.

Bezogen auf die Zielerreichung werden in den jeweiligen Arbeitsbereichen (z.B. Meldewesen) Funktionalität, verarbeitete Datenmengen und Kosten für den Einsatz einer bestimmten IT Lösung, ob im Hardware- oder Softwarebereich sowie deren technische Entwicklungsmöglichkeiten oder Veränderungs- und Anpassungsbedarfe beschrieben. Weitere detaillierte Vorgaben für den Inhalt eines IT Konzeptes ergeben sich aus dem BSI Grundschutzkatalog, der durch die EKD Gesetzgebung zur Orientierung dienen soll.

Wie bei einem Trichter ergeben sich am Ende der Beschreibung der jeweils eingesetzten IT Anwendung bestimmte Standards, deren Einhaltung sowohl durch bestimmtes Verhalten von Mitarbeitenden, die das System nutzen oder durch bestimmte technische Lösungen zwingend einheitlich erforderlich sind, um auf diesem Wege die Daten- und IT-Sicherheit zu gewährleisten.

Dies kann je nach kirchlicher Körperschaft völlig unterschiedlich sein.

Wesentlich ist, dass die im IT Konzept beschriebenen Sachverhalte sowie die eingesetzten Lösungen und die jeweiligen Anwendungen durch die

passenden Standards bindenden Charakter bis hin zu Handlungsanweisungen der Mitarbeitenden haben.

Bezogen auf die bisher im gesamten Bereich der Evangelischen Kirche im Rheinland eingesetzten Referenzlösungen (z.B. Mewis oder Mach) ergeben sich naturgemäß die gleichen Standards.

Vor diesem Hintergrund wird dem IT Rahmenkonzept der Verordnungsrang zugeschrieben.
Zum besseren Verständnis dieser Ausführungen legt die Kirchenleitung die vom Lenkungsausschuss IT bis jetzt erarbeiteten Teile des IT-Rahmenkonzeptes der Landessynode zur Kenntnisnahme vor. Dies hält Die Kirchenleitung aus Informationsgründen für erforderlich, da auf diese Weise der Landessynode eine Vorstellung von dem Inhalt des Rahmenkonzeptes vermittelt werden kann.

Nach dem Gesetzesentwurf kann die Erfüllung der Verpflichtung der kirchlichen Körperschaft gemäß § 7 Absatz 1 zur Erstellung eines IT-Konzeptes erfolgen, indem sie das IT-Rahmenkonzept der Kirchenleitung per Beschluss übernimmt. Dies setzt voraus, dass die technischen Lösungen und Anwendungen des IT-Rahmenkonzeptes der Landeskirche entweder bereits in der kirchlichen Körperschaft eingesetzt werden oder es beabsichtigt ist, die in dem Rahmenkonzept beschrieben Anwendungen und Lösungen zukünftig einzusetzen bzw. die vorhandenen Lösungen entsprechend anzupassen.

Nach Satz 2 der Vorschrift wird den Kirchenkreisen empfohlen, ein einheitliches IT Konzept zu beschließen. Damit wird die Vorgabe des Beschlusses 55 Ziff. 1 der Landessynode 2012, die Vereinheitlichung der Anwendung von Informationstechnologie zu verwirklichen, erfüllt.

Die in dem Gesetzestext untechnisch verwendete Formulierung „empfohlen“ ist der der Kirchenordnung entsprechenden Selbstständigkeit der kirchlichen Körperschaften geschuldet. Im Hinblick auf die Erfüllung des Synodenauftrages ist die Empfehlung allerdings als deutliche Ermunterung zu verstehen. Ziel des Synodenbeschlusses 55 ist nicht die Bewahrung des Status Quo, sondern das Erreichen der Zielgeraden, die eine sinnvolle Vereinheitlichung der Informationstechnologie in der Evangelischen Kirche im Rheinland darstellt.

Durch Satz 2 wird § 7 Absatz 1 Satz 1 insoweit präzisiert, als dass ein einheitliches IT Konzept grundsätzlich auf Kirchenkreisebene nur für alle dem Kirchenkreis angehörenden Kirchengemeinden sinnvoll sein kann. Allerdings haben die Kirchenkreise grundsätzlich nach § 7 die Möglichkeit,

auch eigene, vom IT-Rahmenkonzept abweichende IT-Konzepte in eigener Verantwortung zu erstellen.
Diese müssen dann aber auch für alle dem Kirchenkreis angehörenden Kirchengemeinden, Werke und Einrichtungen gelten.

Diese Regelung ist bewusst so gestaltet worden. Wie die gesamte bisherige Entwicklung der IT in der Evangelischen Kirche im Rheinland, stellt auch die zukünftige Entwicklung einen Prozess dar, der nicht mit einem Schnitt verändert oder angepasst werden kann. Es bleibt deshalb bewusst offen, ob in der näheren oder ferneren Zukunft möglicherweise einmal alle Kirchenkreise ein mit dem IT-Konzept der Kirchenleitung identisches Konzept haben oder nicht.

Wesentlich ist, dass die in dem IT Konzept beschriebenen Anwendungen und Lösungen auch tatsächlich bewusst gelebt werden.

Wegen der hohen Dynamik und ständigen Weiter- bzw. Neuentwicklung im Bereich der angewandten und eingesetzten IT-Lösungen ist die Weiterarbeit an dem IT-Rahmenkonzept logische und zwingende Folge.

Dieser Tatbestand ist in § 5 geregelt. Danach wird die Kirchenleitung, die mit der Erstellung des IT-Rahmenkonzeptes die IT-Sicherheit förmlich gewährleistet, durch die Zuarbeit einer ständigen Kommission unterstützt. Neben den in Absatz 3 genannten Aufgaben der Kommission, die im wesentlich die zur Sicherung der IT der Kirchenleitung obliegenden Aufsichtsaufgaben konkretisieren, hat die Kommission das Rahmenkonzept in einem ständigen Prozess nachzuarbeiten, zu ändern und den neuen IT Lösungen anzupassen.

Der Vorschlag, die Vereinheitlichung der in der Evangelischen Landeskirche eingesetzten IT-Lösungen durch die Übernahme des IT Rahmenkonzeptes der Kirchenleitung kaskadenartig zu gestalten, soll den kirchlichen Körperschaften den immensen Aufwand, der mit der Erstellung eines IT-Konzeptes verbunden ist, erleichtern.

Diese Vorgehensweise hat selbstverständlich auch kostenmäßige Auswirkungen, da die nach dem Rahmenkonzept verwirklichten IT-Lösungen generell für die einzelnen Körperschaften günstiger sein werden, als die nach § 7 Absatz 4 selbst zu finanzierenden Einzellösungen. Dabei spezifiziert § 7 Absatz 3, 2. Halbsatz die gesamtkirchliche Kostenlösung noch einmal. Nicht ausreichend ist lediglich die Übernahme der vorgeschlagenen Referenzlösung, z.B. der Finanzsoftware. Vielmehr verlangt § 7 Absatz 3, 2. Halbsatz, dass auch die Anwendung entsprechend der inhaltlichen Beschreibung des Rahmenkonzeptes erfolgt. Dies bedeutet, dass technische Lösungen, wie z.B. Schnittstellen, die durch nicht dem IT

Rahmenkonzept entsprechende, eigene Zusatzlösungen entstehen, nicht von den Gesamtkosten übernommen werden. (Beispiel: Das IT Rahmenkonzept beschreibt die technische „Zusammenarbeit“ von kidicap p5 und Mach. Es wird aber eine Schnittstelle zu einer anderen kidicap Version oder sogar zu einem anderen Personalabrechnungsprogramm benötigt. Die für die Programmierung der Schnittstelle entstehenden Kosten werden nicht gesamtkirchlich getragen.)

Technische Neuerung im Bereich von Informations- und Kommunikationstechnik erschöpfen sich im Hinblick auf die Kostenentwicklung heute und noch weniger zukünftig, mit der Anschaffung einer neuer Soft- oder Hardware. Vielmehr werden durch jede Veränderung, die auch nur in der Anschaffung eines neuen Handytyps liegen kann, hochkomplizierte, für den Laien kaum noch überschaubare technische Anpassungsbedarfe ausgelöst, die alle kostenverursachend sind.

Deshalb sieht der Gesetzesentwurf in § 6 vor, eine IT-Finanzkommission zu berufen. Als Controlling- und Prüfinstanz hat er für die Kirchenleitung die in den vorangegangenen Absätzen beschriebene technische Entwicklung, die sich in der ständigen Fortschreibung des IT-Rahmenkonzeptes aktualisiert im Auge zu behalten und rechtzeitig bei der Kirchenleitung über außerordentliche Kosten- und Aufwandsentwicklungen zu berichten.
Dabei liegt der Focus der Arbeit nicht nur auf der Kostenbeschreibung des Ist-Zustandes einer IT-Lösung liegen, sondern es sollen insbesondere auch die zukünftigen Kostenentwicklungen mitbedacht werden. Häufig erscheint die Entscheidung für eine bestimmte IT-Lösung im ersten Augenblick preiswert, doch stellt sich erst nach deren Anschaffung heraus, dass so viele technische Lösungen angepasst, neu angeschafft oder umprogrammiert werden müssen, dass diese Kosten den ursprünglichen Anschaffungswert um ein vielfaches übersteigen.

Die IT-Finanzkommission arbeitet unabhängig von der IT-Kommission und legt seine Stellungnahmen der Kirchenleitung auch unabhängig vor. Da die Kirchenleitung gemäß § 4 Absatz 1 regelmäßig über die Fortschreibung des Rahmenkonzeptes beschließt, wird eine Lösung im Rahmenkonzept erst endgültig aufgenommen, wenn die Kirchenleitung über das Votum der IT-Finanzkommission dazu entschieden hat.

Im Rahmen der ständigen Weiterarbeit an dem IT-Rahmenkonzept kann die Kommission der Kirchenleitung gemäß § 5 Absatz 2 Buchst. g) auch Vorschläge für Referenzlösungen unterbreiten, soweit die Voraussetzungen gegeben sind. Für die Beschaffung einer Referenzlösung hat der IT-Finanzkommission im Sinne von § 6 Abs. 3 unter den bereits genannten Gesichtspunkten die Vergleichbarkeit von Angeboten zu prüfen und auch hier insbesondere die Kostenentwicklungsperspektive darzustellen.

Der Gesetzesentwurf nimmt des Weiteren in den §§ 8 und 9 die bereits im geltenden Datenschutzrecht der EKD bestehenden Vorschriften auf, die die zwingende Beteiligung der Datenschutzbeauftragten sowie der Mitarbeitervertretung und den Genehmigungsvorbehalt des Landeskirchenamtes für die Datenverarbeitung im Auftrag regeln. Hier ist also keine neue Rechtslage geschaffen worden.

### 3.3. Struktur eines Rahmenkonzeptes

Als Ergebnis erster Überlegungen zur Struktur eines zukünftigen Rahmenkonzepts konnten folgende Inhalte exemplarisch definiert werden:

1. **Motivation**
2. **Derzeitige Situation**
3. **Kritische Erfolgsfaktoren für die Umsetzung**
4. **Fortschreibung des IT-Konzeptes der Evangelischen Kirche im Rheinland**
5. **Zusammenstellung der IT-Anforderungen**
    - a) Basis Anforderungen
    - b) Anforderungen Groupware
    - c) Anforderungen Meldewesen
    - d) Anforderungen Finanzwesen
    - e) ……
    - f) …….
6. **IT-Verantwortungsstruktur**
    - a) IT-Generalverantwortung
    - b) IT-Kommission
    - c) Organisationsstrukturen
    - d) Betreuungskonzept
7. **IT-Services**
    - a) IT-Basisdienste
        - I. Daten und Speichermanagement
        - II. Kommunikation, Netzwerke, Telekommunikation
        - III. Server und Betriebsumgebung
        - IV. Inventarisierung und Lizenzmanagement
    - b) IT-Ausstattung
        - I. Ausstattung Standorte
            - I.1 Dienststellen mit 1-5 Einzel-Arbeitsplätzen
            - I.2 Dienststellen mit 5 – 10 Arbeitsplätzen
            - I.3 Dienststellen mit bis zu 50 Arbeitsplätzen
            - I.4 Dienststellen mit über 50 Arbeitsplätzen
        - II. Ausstattung Arbeitsplatz
    - c) Fachliche Grundverfahren (Fachanwendungen)
        - I. Meldewesen
        - II. Finanzwesen und Fundraising
        - III. Personal und Verwaltung

IV. Liegenschaftsmanagement und Friedhofsverwaltung
V. Theologie, Bildung und Erziehung

d) Multimediale Öffentlichkeitsarbeit
I. Content Management
II. Web-Publishing
III. Social Media

**8. Datenschutz und Datensicherheit**

a) Datenschutz und –Sicherheit -Grundsatz-
b) Erstellung von IT-Sicherheitskonzepten

**9. Green IT**

a) Nachhaltige Wirtschaftlichkeit von IT-Maßnahmen
b) Kosten / Nutzung
c) Server-Konsolidierung

Im Rahmen eines IT-Rahmenkonzeptes sind bestimmte Anforderungen zu definieren, insbesondere um den gesetzlichen Erfordernissen des Datenschutzes und der IT-Sicherheit Rechnung zu tragen.
Solche Anforderungen wurden im Rahmen der Bearbeitung durch den Lenkungsausschuss und die Projektgruppe entwickelt.
Anlage 7 erläutert, wie die Anforderungen hergeleitet worden sind und enthält Basis-Anforderungen sowie – exemplarisch - spezifische Anforderungen für die Anwendungen Groupware und Meldewesen. Im Rahmen der Erstellung des IT-Rahmenkonzeptes sind weitere spezifische Anforderungen im Blick auf andere Fachanwendungen zu definieren.

## 3.4 Alternatives Modell einer landeskirchenweiten Organisation

Beschluss Nr. 55 der Landessynode 2013 lag eine im Jahre 2012 vorgenommene Analyse des Ist-Zustandes der IT in der Evangelischen Kirche im Rheinland zu Grunde, die einen durchgängig hohen Reformbedarf zeigte. Als wesentliche Schwachpunkte sind zu benennen:

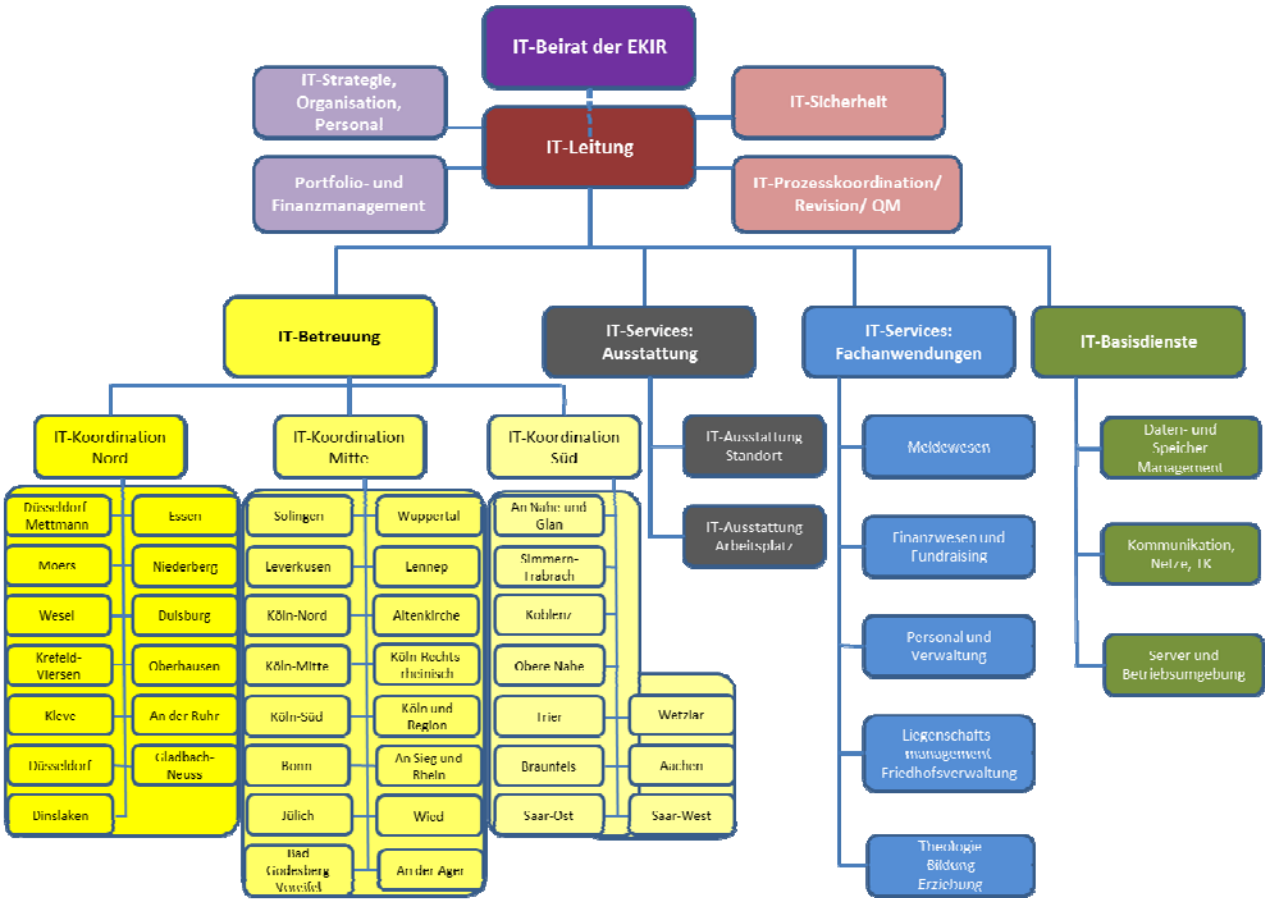
Das Fehlen einer übergeordneten Steuerung mit eindeutiger Abgrenzung von Aufgaben, Verantwortungen und Kompetenzen blockiert eine effiziente Leistungserbringung.

- Kenntnis, Definition und Beachtung von IT-Standards in der Fläche sind nicht gewährleistet. Ein durchgängig zuverlässiger, wirtschaftlicher und rechtssicherer Betrieb ist damit nicht gewährleistet.
- Die personellen Ressourcen sind nicht ausreichend, um den Anspruch einer modernen IT, die sich am Bedarf der Kunden und Mitarbeitenden orientiert, zu erfüllen.
- In ihrer jetzigen dezentralen, heterogenen und intransparenten Organisationsform ist eine zuverlässige Budget- und Kostenplanung nicht möglich.
- Das Problembewusstsein im Blick auf die IT-Aufgaben, -Möglichkeiten und –Gefahren ist nicht hinreichend ausgeprägt.
- Die Nachrangigkeit von Wirtschaftlichkeit in der Definition von Zielen behindert die Wahrnehmung von wichtigen Handlungsbedarfen und deren Priorisierung.
- Die vorhandene IT-Organisation ist nicht innovationsfähig.

Vor dem Hintergrund der definierten fachlichen Anforderungen (IT-Standards) – **Anlage 7** - und einer strukturierten Aufgabenliste (**Anlage 8**) - hat sich der Lenkungsausschuss intensiv mit der Frage auseinander gesetzt, welche Organisation am besten geeignet ist, die Anforderungen, insbesondere in den Bereichen Datenschutz und IT-Sicherheit, einzuhalten, zu pflegen und weiter zu entwickeln, ebenso aber kirchlichen, wirtschaftlichen und betrieblichen Anforderungen gerecht zu werden.

Der Lenkungsausschuss sieht wie die externe Beratung (Kienbaum) folgende Organisationsstruktur als idealtypisch an, die mit gängigen entsprechenden Organisationsstrukturen an Universitäten, in Kommunen und in Landesbehörden vergleichbar ist:

Kirchenleitung (Budget, Strategie, IT-Standards)




Das Ziel und der Anspruch bei dieser neuen IT-Organisation ist die bedarfsgerechte Bereitstellung von Leistungen und Angeboten der IT für die Gesamtorganisation der Evangelischen Kirche im Rheinland. Die gewählte Organisationsform gewährleistet einen zuverlässigen, wirtschaftlichen und rechtssicheren Betrieb. Ermöglicht wird dies durch eine klare Definition und Abgrenzung von Verantwortung und Entscheidungskompetenzen. Auf diese Weise können betriebliche, gesetzliche und kirchliche Rahmenvorgaben bspw. zum Datenschutz oder Sicherheitsbestimmungen effektiv gesteuert und erfüllt werden.

Die neue IT verbindet lokale und zentrale Organisationsvorteile. Die IT-Koordination deckt die lokale Betreuung der Kunden und Mitarbeitenden in den Gemeinden und Kirchenkreisen ab, während die zentralen Organisationseinheiten IT-Services Ausstattung, Fachanwendungen und Basisdienste EKIR übergreifend tätig sind.

Der lokale Charakter in der Betreuung der Gemeinden und Kirchenkreise durch die IT ist weiterhin gewährleistet. Die Nähe und Greifbarkeit der IT durch Kunden und Mitarbeitende schafft Vertrauen und Akzeptanz. Der lokalen IT-Betreuung stehen darüber hinaus Spezialisten zur Verfügung, die

sowohl selbst Aufgaben verantworten und durchführen als auch beratend tätig werden. Dadurch wird das Leistungsportfolio der IT erweitertet, die lokale IT entlastet und der Mangel von IT-Personal auf lokaler Ebene kompensiert.
Wesentliche strukturelle Veränderung bei diesem Modell ist, dass alle IT-Mitarbeitenden Teil einer landeskirchenweiten Organisationseinheit sind, deren Aufgabenwahrnehmung die gemeindliche, die kreiskirchliche und die landeskirchliche Ebene erfasst.
Die neue IT-Organisation macht den großen Stellenwert, den IT bei der effektiven Unterstützung der kirchlichen Arbeit hat, deutlich. Ein einheitliches Auftreten, die Möglichkeit fachlicher Spezialisierung, macht die IT deutlich leistungsfähiger und zu einem leistungsstarken Partner in der Zusammenarbeit. Die IT ist nun in der Lage, Ideen und Entwicklungen in die Gesamtorganisation zu tragen und sich wirkungsvoll bei der Erfüllung des kirchlichen Auftrags einzubringen.
Nachfolgend wird aufgezeigt, auf welche Weise Handlungsbedarfe Niederschlag in der Organisation gefunden haben.

**Lokale Betreuung von Gemeinden und Kirchenkreisen**
Die IT-Koordinatoren sind der jeweiligen IT-Regional-Koordinationsstelle (Nord, Mitte, Süd) unterstellt. Die Zusammenarbeit von Gemeinden, Kirchenkreisen und der Landeskirche erhält durch die Präsenz vor Ort und das Zusammenspiel innerhalb der neuen Organisation eine neue Qualität. Wissen und Kräfte werden gebündelt und zielgerichtet und arbeitsteilig zum Wohle aller eingesetzt, Vertretungen können gewährleistet werden, die Voraussetzungen für eine wirkungsvolle Steuerung externer Dienstleister sind verbessert.
Die lokale IT-Koordination übernimmt die Betreuung der Kunden und Mitarbeitenden auf Gemeinde- und Kirchenkreisebene. Sie kann und soll sich dabei mit den lokal beschäftigten Personen in ihren Regionen abstimmen und die zu erbringenden Aufgaben jeweils in einer optimalen Form organisieren. Die lokalen IT-Betreuer sind daher unter gemeinsamer Leitung als ein Team organisiert. Die Kunden und Mitarbeitenden haben mit der lokalen IT-Koordination einen klar definierten Eingangskanal in die IT. Anfragen können gezielt weitergeleitet und so schneller bearbeitet werden.
Die IT-Koordination der Kirchenkreise betreut die Gemeinden und Kirchenkreise nach einem mit dem jeweiligen Kirchenkreis und der Bereichsleitung IT-Betreuung abgestimmten Konzept. Für den Fall, dass die lokale IT-Koordination eines Kirchenkreises gewisse Leistungen nicht selbst erbringt, übernimmt sie die Steuerung der ausgewählten Dienstleister und gibt die entsprechenden Rahmenbedingungen vor. Auf diese Weise können lokale Bedürfnisse und Anforderungen besser berücksichtigt werden. Im Vertretungsfall übernimmt die IT-Koordination ebenfalls die IT-Koordination eines benachbarten Kirchenkreises. Dadurch wird eine durchgängige Betreuung der Kunden und Mitarbeitenden gewährleistet. Etwaige

kirchenkreisübergreifende Aufgaben werden auf regionaler Ebene der jeweiligen IT-Koordination (Nord, Mitte, Süd) koordiniert und gesteuert. Die regionalen Bereichsleitungen der IT-Koordination können in der übergeordneten Perspektive besser Engpässe in der IT-Betreuung erkennen und gezielt Maßnahmen zur Behebung einleiten und steuern.

**IT-Führung**

Ein wesentlicher Aspekt der neuen Organisation ist die Schaffung einer klaren Verantwortung für die IT in der Evangelischen Kirche im Rheinland. Die IT-Leitung ist die oberste Entscheidungsinstanz und für die Gesamtstrategie verantwortlich. Die neue Organisation schafft der IT-Leitung den nötigen Freiraum, die IT-Strategie als das wichtigste Führungselement zu erarbeiten. Nur so gelingt es, die IT an den aktuellen und künftigen Bedürfnissen der Kunden und der Gesamt-Organisation Evangelische Kirche im Rheinland auszurichten, sowie die Effizienz und Effektivität der IT-Organisation zu steigern. Die IT-Leitung muss die Möglichkeiten und Chancen moderner IT für die Evangelische Kirche im Rheinland aufzeigen und die Innovation stetig vorantreiben. Dazu muss die IT-Leitung aktuelle Entwicklungen in Technologien und Methoden beobachten, deren Bedeutung für die Evangelische Kirche im Rheinland ableiten und in die IT-Strategie einfließen lassen.

Alle Berichtslinien der verschiedenen IT-Bereiche laufen in dieser Funktion zusammen. Die IT „spricht“ mit einer Stimme in die Gesamtorganisation und sendet so seltener widersprüchliche und/oder redundante Signale. Klar abgegrenzte Verantwortlichkeiten und Schnittstellen sorgen für Transparenz hinsichtlich der Zuständigkeit.

Der IT-Leitung stehen Stabs- und Querschnittsfunktionen zur Seite. Die Kompetenzbündelung in diesen zentralen Organisationseinheiten hat ihre Begründung in der Bereitstellung von übergreifendem Wissen und Erfahrung in den besetzten Themenfeldern für die gesamte IT-Organisation. Die Stabs- und Querschnittsfunktionen stehen allen Bereichen beratend zur Verfügung und tragen in ihren jeweiligen Themengebieten die Gesamtverantwortung für die IT-Organisation. Das spezielle Aufgaben- und Leistungsportfolio der Organisationseinheiten ist auf diese Weise deutlich sicht- und nutzbar für Kunden und Mitarbeitende der Evangelischen Kirche im Rheinland sowie für die anderen IT-Organisationseinheiten. Informationen fließen schneller und gehen weniger verloren aufgrund verringerter und sauberer Schnittstellen. Die benötigten Kennzahlen sind für die Bereichsleitungen leichter zugänglich.

Zusammenfassend handelt es sich bei der Organisation der IT-Führung mit IT-Leitung, Stabstellen und Querschnittsfunktionen um die Demand Seite der neuen IT der Evangelischen Kirche im Rheinland. Es werden alle strategischen und taktischen Aufgaben der IT-Organisation zusammengefasst. Die Interaktion zwischen den Kunden und

Mitarbeitenden und den Leistungserbringern wird durch die Führungsorganisation gesteuert und koordiniert.

**Politische Steuerung**
Der IT-Beirat übernimmt die Bindegliedfunktion zwischen IT-Leitung und Kirchenleitung bzw. Synode. Dadurch ist ein stetiger Austausch zwischen den Führungsgremien der Kirche und der IT möglich. Veränderte Rahmenbedingungen in Bezug auf kirchliche und gesellschaftliche Erfordernisse können auf diesem Weg schnell Einfluss und Niederschlag in die Planung und Ausrichtung der IT-Strategie finden. Der Beirat steht der IT-Leitung als Beratungsgremium zur Verfügung. Diese Funktion bietet eine unabhängige Kontrolle für die Kunden und Mitarbeitenden der Evangelischen Kirche im Rheinland, damit die IT sich weiterhin an ihren Anforderungen orientiert.

**Bildung von Kompetenzcentern**
Es werden mit den Bereichen IT-Services Ausstattung, Fachanwendungen und Basisdienste zentrale Organisationseinheiten geschaffen, die in der Funktion eines Kompetenzcenters Leistungen in Form von IT-Services für die gesamte Evangelische Kirche im Rheinland überregional erbringen. Dadurch bietet sich die Möglichkeit zur Vereinheitlichung der IT und zur Homogenisierung der Anwendungslandschaften. Hierfür beschäftigt jede Organisationseinheit fachlich spezialisierte Mitarbeitende. Vorhandenes Wissen kann so zielgerichteter eingesetzt bzw. über höhere Spezialisierungsgrade vertieft und neu erworben werden. Die Spezialisierung der Mitarbeitenden ermöglicht es besser darüber zu entscheiden, ob eine IT-Leistung selbst oder fremd erbracht werden soll. Ebenso können selbstentwickelte Lösungen besser in der Fläche verteilt und auf die speziellen Anforderungen einzelner Kunden- und Anwendungsgruppen angepasst werden.
Jede zentrale Organisationseinheit hat seine eigene, entscheidungsbefugt handelnde Leitung. Dadurch erfolgt die Kommunikation zur IT-Leitung gebündelt. Informationen können besser gesteuert und flächendeckend verteilt werden. Die Mitarbeitenden dieser zentralen Organisationseinheiten stehen der lokalen IT-Koordination beratend zur Seite bzw. steuern diese fachlich im Rahmen der Erbringung einzelner IT-Services bzw. notwendiger vor Ort zu erbringender Aufgaben. Durch die Einbindung der lokalen IT-Koordination profitieren die zentralen Organisationseinheiten von dezentralem Fachwissen. Die Zusammenarbeit fördert die Akzeptanz in der Fläche. Weiterhin bedeutet die Auslagerung bestimmter Services in übergeordnete Organisationseinheiten einen Zeit- und Ressourcengewinn für die lokale IT-Koordination. Durch die höhere Verfügbarkeit der IT-Koordination erhöht sich die Zufriedenheit der Kunden und Mitarbeitenden in den Gemeinden und Kirchenkreisen.

Das gebündelte Fachwissen hinsichtlich der Kompetenzfelder steht an einem Ort gebündelt und transparent zur Verfügung. Es wird so verhindert, dass die IT-Leistungen redundant erbracht werden und/oder nicht sicht- und nutzbar für andere Gemeinden oder Kirchenkreise sind. Die zentralen Organisationseinheiten stehen der lokalen IT-Koordination darüber hinaus als 2nd Level-Support zur Verfügung und koordinieren ihrerseits die Kommunikation und Zusammenarbeit mit den Herstellern. Die fachlichen Ressourcen können auf diese Weise besser genutzt und positive Skaleneffekte erzielt werden. Der Einkauf von Dienstleistungen oder Hard- und Software kann über die zentralen Organisationseinheiten besser gesteuert werden. Dienstleister können effektiver analysiert und dahingehend bewertet werden, ob sie die Anforderungen und Standards der Evangelischen Kirche im Rheinland erfüllen. Die zentralen Organisationseinheiten können spezifische Entwicklungen, Fortschritte und Trends besser analysieren und den Nutzen für die Evangelische Kirche im Rheinland ableiten. Auf diese Weise ist ein effektiveres Innovationsmanagement möglich.
Mit der Einrichtung von zentralen Organisationseinheiten ist es darüber hinaus möglich, für bestimmte IT-Services ein höheres Niveau in der Datensicherung und Business Continuity zu erreichen. Insbesondere den stetig steigenden Anforderungen im Bereich Datenschutz und IT-Sicherheit kann auf diese Weise adäquat begegnet werden.
Die Organisationseinheiten sind verantwortlich für das Finanzmanagement ihres Kompetenzbereichs. Dadurch lassen sich die Budgets und Kosten der einzelnen Organisationseinheiten besser planen, analysieren und verfolgen.

**Schlanke Organisation**
Die neue Organisation zeichnet sich durch eine geringe Anzahl von Hierarchiestufen aus. Die einzelnen Organisationseinheiten sollen personell möglichst klein gehalten werden, um schnell und flexibel auf sich verändernde Herausforderungen reagieren zu können. Ziel ist in den Organisationseinheiten die Aufgabenerledigung aus einer Hand. Arbeitsabläufe werden so verkürzt und kundenfreundlich gestaltet. Die Mitarbeitenden haben dadurch zwar umfangreiche Aufgaben zu erfüllen, allerdings können sie selbstständiger arbeiten und tragen mehr Verantwortung.
Der Lenkungsausschuss ist überzeugt davon, dass dieser Organisationsvorschlag grundsätzlich idealtypisch geeignet ist, die von der Landessynode 2013 beauftragte durchgreifende Verbesserung der IT in der Evangelischen Kirche im Rheinland insgesamt zu leisten.
Organisationen vergleichbarer Größe sind vergleichbar aufgestellt. Das Modell darf als im öffentlichen Sektor üblich bezeichnet werden.
Auch die Fa. Kienbaum erachtet dieses Modell als optimale Organisation.
Der Lenkungsausschuss hat sich trotz der aus seiner Sicht unbestreitbaren Vorteile des Organisationmodells dazu entschlossen, dieses Modell nicht

weiter zu detaillieren und zur Beschlussfassung zu empfehlen, weil er eine Umsetzung zurzeit und bis auf weiteres nicht für realistisch hält.
Es wird erwartet, dass die Schaffung einer homogenen, auf allen Ebenen tätigen IT-Organisation auf keine hinreichende Akzeptanz stoßen würde. Eine bis in die Gemeinde wirkende Organisation, bei der die Leitungsgremien, alle beruflich und ehrenamtlichen Mitarbeitenden „Kunden“ der Organisation sind, hätte hohen Neuigkeitswert. Die weit reichende Verlagerung von Entscheidungskompetenzen weg von den Gemeinden und Kirchenkreisen würde aller Voraussicht nach erhebliche Widerstände auslösen. Vor diesem Hintergrund erscheint es nicht realistisch, die schwierige Aufgabe, eine idealtypische Organisation als neues synodales Element in absehbarer Zeit „aus dem Boden zu stampfen“ und ihre Kompetenzen fruchtbar zu machen.
Außerdem ist ein seriöser Vergleich der Wirtschaftlichkeit der Ist-Situation und der Aufgabenwahrnehmung durch die idealtypische Organisation ist nicht möglich. Zum einen hat die Analyse gezeigt, dass IT-Aufgaben in den derzeitigen heterogenen Strukturen nur teilweise und in unterschiedlicher Tiefe wahrgenommen werden. Zum anderen besteht keine Transparenz hinsichtlich der qualitativen und quantitativen Ressourcen (Personal- und Sachmitteleinsatz), die derzeit im IT-Sektor aufgewendet werden.
Ohne eine belastbare vergleichende Betrachtung von Nutzen und Kosten kann angesichts von Einsparungszwängen keine breite Bereitschaft erwartet werden, eine neue IT-Organisation dieser Art zu etablieren.
Aus den genannten Gründen hat sich der Lenkungsausschuss dafür ausgesprochen, die von der Landessynode vorgegebenen Ziele im Bereich der Informationstechnologie durch die vorgeschlagene gesetzliche Regelung, insbesondere durch die Verpflichtung jeder kirchlichen Körperschaft ein IT-Konzept nach Maßgabe des IT-Rahmenkonzepts aufzustellen, zu verfolgen.

## 4. Beratungsergebnisse der beteiligten Ausschüsse und der Kirchenleitung

Der Entwurf einer Vorlage für die Landessynode, der die Verabschiedung des Kirchengesetzes über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland zum Beschlussgegenstand hatte, ist von der Kirchenleitung in ihrer Sitzung am 20.09.2013 an den Ständigen Ausschuss für Kirchenordnung und Rechtsfragen (federführend), an den Ständigen Finanzausschuss sowie an den Ständigen Innerkirchlichen Ausschuss zur Mitberatung überwiesen worden.

Die Voten der beteiligten Ständigen Ausschüsse sind als **Anlage 4, 5 und 6** beigefügt.

Zusammenfassend lässt sich feststellen, dass die beteiligten Ausschüsse übereinstimmend zu der Auffassung gelangt sind, dass die Verabschiedung eines Kirchengesetzes über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland auf der Landessynode 2014 verfrüht wäre. Vor einer entsprechenden Entscheidung wird eine breitere Information und Beteiligung von Fachleuten und Entscheidungsträgern auf kreiskirchlicher und gemeindlicher Ebene im Rahmen regionaler Fachkonferenzen für erforderlich gehalten. Diese Konferenzen dienen dem Zweck, sowohl Akzeptanz für die Notwendigkeit des Vorhabens insgesamt zu erreichen, als auch ein Forum zu schaffen, auf dem insbesondere ein Austausch über die Aspekte Wirtschaftlichkeit, IT-Sicherheit und Verbindlichkeit stattfinden kann. Ggf. können Anregungen und Vorschläge aus den regionalen Fachkonferenzen im Rahmen der Vorbereitung der Beschlussfassung der Landessynode 2015 berücksichtigt werden.

Die Kirchenleitung hat sich in ihrer Klausurtagung am 18/19.10. ebenfalls für eine Aussetzung der Beschlussfassung und die Veranstaltung regionaler Fachkonferenzen ausgesprochen.. Sie ist ferner der Auffassung, dass das IT-Rahmenkonzept im Laufe des Jahres 2014 erstellt werden soll, um die Informationsbasis für die Beschlussfassung der Landessynode 2015 zu verbessern.

## 5. Kosten

Für die erstmalige Erstellung des IT-Rahmenkonzepts besteht ein Personalbedarf von 3 IT-Fachkräften und einer juristischen Begleitung über einen Zeitraum von 7 Monaten. Das ergibt geschätzte Personalkosten von ca. 200.000 Euro.

Für die Tätigkeit des IT-Lenkungsausschusses und die Durchführung der regionalen Fachkonferenzen werden die Kosten auf ca. 10.000 Euro geschätzt.

Damit ergeben sich Gesamtkosten in Höhe von ca. 210.000 Euro.

**Vorschlag der Kirchenleitung:**

**Überweisung an den Ausschuss für Kirchenordnung und Rechtsfragen (II) – federführend –, an den Innerkirchlichen Ausschuss (IV) und an den Finanzausschuss (VI)**

**Anlage 1**

EVANGELISCHE KIRCHE IM RHEINLAND

# Auszug
# aus dem Protokoll der Landessynode
# der Evangelischen Kirche im Rheinland
# vom 12. Januar 2013

---

## Informationstechnologie

**Beschluss 55:**

1. *Die Kirchenleitung wird beauftragt, der Landessynode 2014 einen Beschlussantrag zu unterbreiten, wie die von der Landessynode 2012 angestrebte Vereinheitlichung der Anwendung von Informationstechnologie in der Evangelischen Kirche im Rheinland verwirklicht wird. Ziel ist dabei, den gesetzlichen Schutzbedarf von Informationen zu erfüllen und gleichzeitig Wirtschaftlichkeit und Qualität des IT-Einsatzes nachhaltig sicherzustellen. Der künftige strukturelle und rechtliche Rahmen, in dem sich der operative Betrieb vollzieht, ist festzulegen.*

   *Dabei sind insbesondere im Jahre 2013 zu definierende IT-Standards, das novellierte Datenschutzgesetz sowie weitere gesetzliche Vorgaben und die Ergebnisse aus den Beratungen zur Verwaltungsstrukturreform einzubeziehen. Im Rahmen der Weiterarbeit sollen die von der Arbeitsgruppe IT in Bearbeitung des Beschlusses Nr. 75 der Landessynode 2012 erzielten Ergebnisse mit bedacht werden.*

2. *Zur Begleitung und Überwachung der Erledigung des Auftrages beruft die Kirchenleitung einen Lenkungsausschuss, der ihr die Ergebnisse vorlegt.*

   *Dem Lenkungsausschuss arbeiten das Landeskirchenamt und kirchliche Kompetenzträger außerhalb des Landeskirchenamtes – insbesondere IT-Verantwortliche aus den Kirchenkreisen – zu. Außerdem wird die Erledigung des Auftrages durch externe Beratung unterstützt und die Datenschutzbeauftragte wird eingebunden.*

   *Der Lenkungsausschuss soll nicht mehr als sechs Mitglieder haben, darunter je ein Mitglied des Ständigen Innerkirchlichen Ausschusses, des Ständigen Finanzausschusses und des Ständigen Ausschusses für Kirchenordnung und Rechtsfragen und eine Superintendentin oder ein Superintendent sowie der Vizepräsident oder eine von ihm zu benennende Vertretung. Mindestens eine ehrenamtliche Mitarbeiterin bzw. ein ehrenamtlicher Mitarbeiter muss dem Lenkungsausschuss angehören. Die Kirchenleitung bestimmt den Vorsitz.*

3. *Für die Erfüllung des Auftrages wird ein Budget in Höhe von 81.000 Euro bereitgestellt. Die Finanzierung erfolgt entsprechend dem Anteil der Kirchengemeinden und dem Anteil der Landeskirche am Kirchensteueraufkommen (89,9%/10.1%).*

*(Mit Mehrheit,*
*bei einigen Gegenstimmen und einigen Enthaltungen)*

**Anlage 2**

# Auszug
# aus dem Protokoll der Landessynode
# der Evangelischen Kirche im Rheinland
# vom 13. Januar 2012

---

## Informationstechnologie

**Beschluss 75:**

1. *Die Kirchenleitung wird beauftragt, der Landessynode 2013 die Eckpunkte eines IT-Konzeptes für die Evangelische Kirche im Rheinland mit dem Entwurf eines Projektplanes zu seiner Implementierung und einer Kostenschätzung zur Entscheidung vorzulegen.*

   *Ziel ist die Schaffung einer einheitlichen IT-Struktur, die einen unter Effektivitäts- und Effizienzgesichtspunkten optimierten Einsatz von Informationstechnologie in der gesamten Landeskirche sicher stellt, auch mit Rücksicht auf die steigenden Anforderungen an IT-Sicherheit und Datenschutz.*

2. *Für die Vorplanungsphase werden bis zu 165.000,00 € bereitgestellt.*

   *Die Kosten werden zu 89,9 % aus der gesamtkirchlichen Umlage und zu 10,1 % aus der landeskirchlichen Umlage finanziert.*

3. *Die Kirchenleitung wird beauftragt, für die bis zur Landessynode 2013 zu leistenden Arbeiten eine Arbeitsgruppe zu berufen. Die Gruppe soll möglichst nicht mehr als 15 Mitglieder haben. Dabei sollen der Ständige Innerkirchliche Ausschuss, der Ständige Finanzkommission, der Ständige Ausschuss für Kirchenordnung und Rechtsfragen, die Superintendentinnen und Superintendenten, Verwaltungsfachleute sowie mindestens fünf IT-Verantwortliche aus Kirchengemeinden, Kirchenkreisen und aus anderen Landeskirchen vertreten sein.*

4. *Damit sind die Anliegen der Anträge der Kreissynoden Niederberg und Wuppertal betreffend Einheitliches IT-Konzept für Verwaltungsaufgaben bzw. betreffend Entwurf eines IT-Gesetzes (Beschlüsse 4.22 bzw. 4.37 der Landessynode 2011) aufgenommen.*

*(Mit Mehrheit)*

**Anlage 3**

| **Lenkungsausschuss IT/Beschluss Nr. 55 der Landessynode 2013** | | | | | |
|---|---|---|---|---|---|
| 1. | Herr | Superintendent | Christian | Weyer | Vorsitz |
| 2. | Herr | | Peter | Berger | Innerkirchlicher Ausschuss |
| 3. | Herr | | Jens | Bublies | Ausschuss für Kirchenordnung und Rechtsfragen |
| 4. | Herr | Pfarrer | Wolfgang | Meyer | Finanzausschuss |
| 5. | Herr | Vizepräsident | Dr. Johann | Weusmann | |

**Anlage 4**

Votum des Ständigen Ausschusses für Kirchenordnung und Rechtsfragen vom 11./12.10.2013

Auszug aus der
noch nicht genehmigten Niederschrift
über die Sitzung am 11./12.10.2013

## 4. Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland

Die Vorsitzende begrüßt Herrn Lammertz, Mitarbeitender im Landeskirchenamt, der in die Vorlage einführt.

Zur Verwirklichung der Vereinheitlichung der Anwendung von Informationstechnologie in der Ev. Kirche im Rheinland hat die Kirchenleitung einen Lenkungsausschuss einberufen. Zur Unterstützung der Arbeit des Lenkungsausschusses wurde eine Projektgruppe gebildet, die sich mit der Definition von IT-Anforderungen auseinander setzen sollte. Die komplexen und größtenteils technisch orientierten Anforderungen können nicht in einem Gesetz geregelt werden. Es ist daher erforderlich, IT-Rahmenkonzepte zu entwickeln, mit denen diese Anforderungen beschrieben und technischen Lösungen zugeführt werden.

Das vorliegende Gesetz sieht vor, dass alle kirchlichen Körperschaften ein IT-Konzept zu erstellen haben. Es wird empfohlen, dass die Kreissynode für den Kirchenkreis, seine Werke und Einrichtungen und die ihr angehörenden Kirchengemeinden ein einheitliches IT-Konzept beschließt.
Alle kirchlichen Körperschaften können sich aber auch dem IT-Rahmenkonzept der Evangelischen Kirche im Rheinland anschließen, wenn sie die dem IT-Rahmenkonzept entsprechenden Lösungen und Anwendungen einsetzen.

Auf die Frage des Ständigen Ausschusses, was man unter „verbindliche Referenzlösungen“ versteht (§ 4 Abs. 3 der Gesetzesvorlage), antwortet Herr Lammertz, dass es sich dabei einheitliche Programme handelt, die - gesamtkirchlich gesehen - von Interesse sind (z.B.: im Bereich Meldewesen und NKF).

Der Ständige Ausschuss weist darauf hin, in § 6 Abs. 3 der Gesetzesvorlage die Wörter „gemäß § 4 Absatz 2“ durch die Wörter „gemäß § 4 Absatz 3“ zu ersetzen.

Der Ständige Ausschuss empfiehlt, § 7 Abs. 3 der Gesetzesvorlage sprachlich zu überarbeiten. Auf Nachfrage, wie hoch die Kosten für eine einheitliche IT-Lösung sein werden, entgegnet Herr Lammertz, dass die Höhe der Kosten zur Zeit nicht genannt werden kann. Im Rahmen einer Umlage würden die Kosten für eine einheitliche IT-Lösung erhoben (vgl. Meldewesen, NKF).

Herr Dr. Weusmann ergänzt, dass die kirchlichen Körperschaften einige IT-Anforderungen (z.B. im Bereich Meldewesen, Groupware) jetzt schon erfüllen müssten, um den gesetzlichen Vorgaben (z.B. Datenschutzgesetz der EKD) zu entsprechen.
Die Superintendentinnen- und Superintendentenkonferenz hat die Gesetzesvorlage diskutiert und hat folgende Empfehlung ausgesprochen:
Die Landessynode 2014 nimmt das Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland zur Kenntnis. Es wird empfohlen, für das Kirchengesetz auf Regionalkonferenzen zu werben. Die Landessynode 2015 soll abschließend über das Kirchengesetz entscheiden.

Der Ständige Ausschuss schließt sich der Stellungnahme der Superintendentinnen- und Superintendentenkonferenz an. Bezüglich der Umsetzung der Verwaltungsstrukturreform in Kirchenkreisen und Kirchengemeinden sollten Übergangslösungen im Blick gehalten werden.

Der Ständige Ausschuss für Kirchenordnung und Rechtsfragen nimmt dankbar das Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland zur Kenntnis und befürwortet dessen Umsetzung.

Der Ständige Ausschuss für Kirchenordnung und Rechtsfragen empfiehlt der Kirchenleitung, dass die Landessynode 2014 das Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland zur Kenntnis nimmt. Auf Regionalkonferenzen soll das Kirchengesetz den Kirchengemeinden und Kirchenkreisen vorgestellt werden. Die Landessynode 2015 soll abschließend über das Kirchengesetz entscheiden.

(einstimmig)

**Anlage 5**
Votum des Ständigen Finanzausschusses vom 17.10.2013

EVANGELISCHE KIRCHE IM RHEINLAND

LKA 14/11/2013

**Auszugsweise Abschrift aus der Verhandlungsniederschrift**
**des Ständigen Finanzausschusses vom 17. Oktober 2013**
*(wird für die Akten besonders vorgelegt)*



## 8. Informationstechnologie – Erledigung des Beschlusses 55 der Landessynode 2013

Kirchenrechtsdirektorin Schwab und Herr Lammertz erläutern die Vorlage. Der Ausschuss für Kirchenordnungs- und Rechtsfragen hat empfohlen, auf Regionalkonferenzen für das Gesetz vorzustellen und damit um Akzeptanz zu werben.

In der anschließenden Diskussion werden folgende Punkte angesprochen:

- Diskussionsbedarf ist groß und kann nicht bis zur nächsten Landessynode umfassend geklärt werden
- Mittlere Ebene muss in die Lage versetzt werden, Werbung für das Gesetz zu betreiben und die Sinnhaftigkeit herauszustellen (datenschutzrechliche Voraussetzungen)
- Regionalkonferenzen nutzen, um die Fachleute und die Entscheidungsträger auf den verschiedenen Ebenen für das Gesetz und dessen Hintergrund zu sensibilisieren

**Beschluss 8:**

Der Finanzausschuss nimmt den Entwurf des „Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland" zur Kenntnis (Anlage beim Hauptprotokoll).

Er befürwortet dass auf Regionalkonferenzen vor einer endgültigen Entscheidung durch die Landessynode das Gesetz den Fachvertretern und den Entscheidungsträgern der verschiedenen Ebenen vorgestellt wird.

**(einstimmig)**

99-11-0

**Anlage 6**
Votum des Ständigen Innerkirchlichen Ausschusses vom 07.11.2013

**STÄNDIGER INNERKIRCHLICHER AUSSCHUSS**

Auszug aus der
noch nicht genehmigten Niederschrift
der Klausurtagung vom 07.-08.11.2013

---

## TOP 3 Vorlage Landessynode 2014 – Informationstechnologie

Herr Lammertz erläutert Zustandekommen und Beratungsverlauf zur Vorlage „Informationstechnologie".
Auf Grundlage des Synodenbeschlusses 2012 war die Arbeitsgruppe IT mit der Erhebung aller notwendigen Daten beschäftigt. Es wurden Anforderungen definiert und in Kategorien eingeteilt. Standards wurden ermittelt – hier stehen 143 Anforderungen, die notwendig sind, den gesetzlichen Regelungen Rechnung zu tragen.
Um Regelungen zu schaffen, soll ein IT-Rahmenkonzept geschrieben werden, das flexibel bleibt durch permanente Fortschreibung und sukzessive Vervollständigung.
Die Kirchenkreise könnten dieses Konzept übernehmen oder eigene Konzepte anwenden, die aber die Mindeststandards sicherstellen müssen. Dann würde das eigene System durch den Kirchenkreis zu finanzieren sein, nicht durch die landeskirchliche Umlage.

Nach dem bisherigen Beratungsweg wurde vorgeschlagen, das Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland der Landessynode 2014 zur Kenntnis zu geben und die Beschlussfassung bis zur Synode 2015 auszusetzen.
Bis zur Synode 2015 soll die umfangreiche Thematik in Fachkonferenzen gemeinsam mit Kirchenkreisen und Kirchengemeinden diskutiert werden und die Erfahrungen und Ergebnisse bei der Beschlussfassung berücksichtigt werden. Die Fachkonferenzen sollen durch den Lenkungsausschuss vorbereitet und durchgeführt werden, der auch das Rahmenkonzept fortschreiben wird.

Der Innerkirchliche Ausschuss sieht in diesem Verfahrensvorschlag einen guten Weg.
Er empfiehlt:

- Die grundsätzliche Vermittlung, dass Sicherheit im Vordergrund steht;
- Eine gute Argumentation in Bezug auf die Aufgabenkritik;
- Vermittlung, wie sich das Verfahren wirtschaftlich darstellt;

- § 7 Absatz 1 zu verstärken bzw. mit Nachdruck zu belegen, um die Erstellung eines IT-Konzeptes unter Beachtung des IT-Rahmenkonzeptes verpflichtender zu regeln.

**Beschluss 3**

1. Der Ständige Innerkirchliche Ausschuss schließt sich dem Beschluss des Ständigen Ausschusses für Kirchenordnung und Rechtsfragen an und empfiehlt der Kirchenleitung, dass die Landessynode 2014 das Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der Evangelischen Kirche im Rheinland zur Kenntnis nimmt. Auf Fachkonferenzen soll das Kirchengesetz den Kirchengemeinden und Kirchenkreisen vorgestellt werden. Die Landessynode 2015 soll abschließend über das Kirchengesetz entscheiden.
2. Der Ständige Innerkirchliche Ausschuss empfiehlt, die inhaltliche Vermittlung der Wirtschaftlichkeit und die Aspekte der Sicherheit in den Vordergrund zu stellen. Er regt an,
   § 7 Abs. 1 verpflichtender zu regeln.
3. Das Beratungsergebnis des Ständigen Ausschusses für Kirchenordnung und Rechtsfragen vom 11./12.10.13 wird zur Kenntnis genommen.

(bei einer Enthaltung so beschlossen)

**Anlage 7 a**

Anlage 7 a

# Beschreibung der Basisanforderungen für IT Systeme in der Evangelischen Kirche im Rheinland

**Hinweis:**
**Dieses Dokument befindet sich im Entwurfsstadium.**

# *Inhalt*

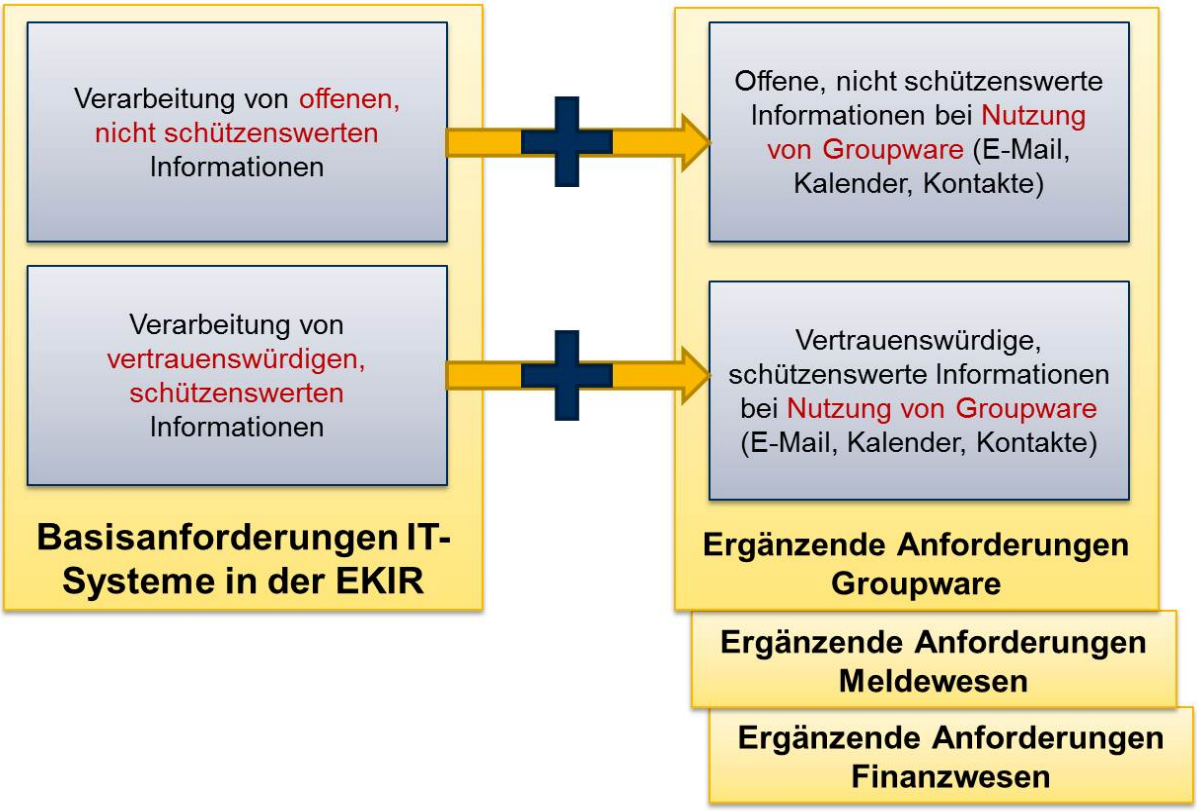
## *Einführung*

Die Informationstechnologie und damit IT-Systeme unterliegen einer ständigen Veränderung. Die Evangelische Kirche im Rheinland (EKiR) steht vor der Herausforderung, Werkzeuge bereitzustellen, die einen wirtschaftlichen, rechtssicheren, funktionsorientierten und anwenderfreundlichen Einsatz von IT-Systemen beherrschbar machen. Vor diesem Hintergrund wurden IT-Standards zusammengetragen und dokumentiert, die nahezu allesamt auch heute schon bei Betrieb und Nutzung von IT innerhalb der EKiR bestehen und relevant sind. Teilweise aus Unkenntnis dieser Betriebs- und Nutzungsanforderungen, teilweise aus fehlenden organisatorischen Voraussetzungen und teilweise auch aus weiteren Gründen wurden viele dieser IT-Standards nicht konsequent beachtet.

Dieses Dokument und die weiteren Dokumente des „IT-Standard Baukastens“ sollen eine Grundlage sein, zum einen Anforderungen an die IT-Organisation abzuleiten, die so zu gestalten sind, dass die Einhaltung der Standards gewährleistet ist, und zum anderen allen Nutzerinnen und Nutzern sowie heutigen Betreibern von IT in der EKiR eine Hilfestellung bei Auswahl, Nutzung und Betrieb ihrer IT-Systeme bieten.

### *Baukastensystem IT-Standards EKiR*

Der Aufbau des Baukastensystems der IT-Standards in der EKiR ist in folgendem Schaubild dargestellt:



Der Baukasten differenziert grundsätzlich zwei Bereiche:

- Basisanforderungen: Diese Anforderungen gelten für alle in der EKiR eingesetzten IT-Systeme.

- Ergänzende Anforderungen: Diese beziehen sich direkt auf die einzelnen Softwarelösungen oder abgegrenzte IT-Systeme. Aktuell wurden ergänzende Anforderungen für die Bereiche Groupware (E-Mail, Kalender, Kontaktdaten), Meldewesen (Mewis) und Finanzwesen (Mach NKF) dokumentiert.

### *Offene oder schützenswerte Informationen*

Innerhalb dieser beiden Bereiche (Basis und Ergänzung) wird weiterhin differenziert, ob es sich um die Verarbeitung vertrauenswürdiger und schützenswerter Informationen handelt oder offene Informationen im IT-System verarbeitet werden:

- Offene Informationen sind Inhalte, die selbst durch missbräuchliche oder ungewollte Veröffentlichung oder Weitergabe keinen persönlichen oder institutionellen Schaden verursachen und keine ungewollten Rückschlüsse auf die persönlichen, sozialen oder sachlichen Verhältnisse zu lassen. Bespiele sind Pressemitteilungen, Newsletter oder Veranstaltungshinweise.

- Schützenswerte Informationen sind alle Daten, bei denen im Falle eines Missbrauchs oder Missachtens der Vertraulichkeit ein Schaden entstehen kann. Dieser Schaden kann wirtschaftlicher, politischer, imageschädigender, ethischer oder existenzbedrohender Art sein. Darüber hinaus handelt es sich um Inhalte, die Rückschlüsse auf die persönlichen, sozialen oder sachlichen Verhältnisse einer Person zulassen. Insbesondere zu nennen sind hier personenbezogene Daten, Seelsorgedaten, steuerliche Daten und sonstige schützenswerte Daten wie Ausschreibungen. Gemeinsam ist diesen Daten, dass man sie in Papierform in geschlossenen Räumen oder Schränken aufbewahren würde.

### *Verbindlichkeitsgrade*

Die Unterscheidung in offene und schützenswerte Informationen ist vor allem relevant im Hinblick auf die Verbindlichkeit einer Anforderung, die jeweils in den Stufen Muss, Soll oder Kann dokumentiert wurde. Die Auswirkungen sind nachstehend erläutert:

- Eine Muss-Anforderung bedeutet, dass eine Forderung unbedingt erfüllt sein muss und nicht verzicht- oder verhandelbar ist, i.S. einer rechtlichen, technischen und funktionalen Mindestanforderung. Beispiel: ein IT-System muss den Vorgaben des Datenschutzes gerecht werden.

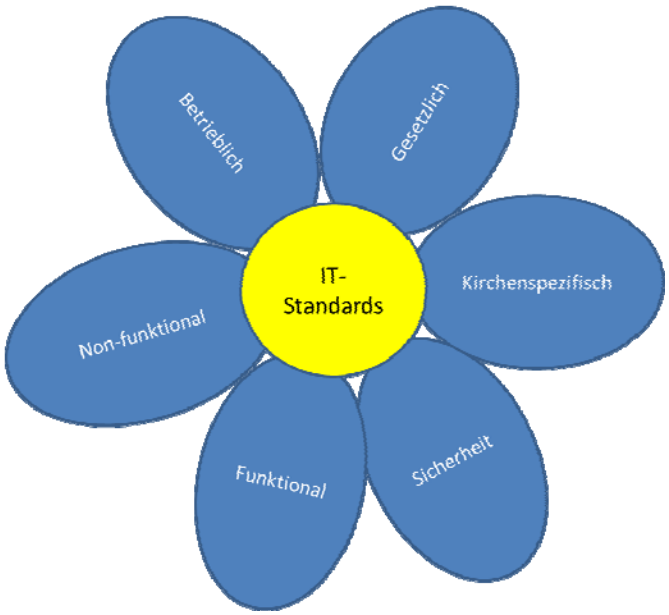
- Die Soll-Verbindlichkeit ist eine schwächere Muss-Anforderung des IT-Systems. Die Anforderung ist nicht verbindlich, aber unbedingt wünschenswert („Quasi-Muss“). Die Erfüllung der Anforderung zieht einen Mehrwert und Nutzen nach sich.

- Die Kann-Verbindlichkeit ist die schwächste Form hinsichtlich der Erfüllung einer Anforderung. Sie ist in der Regel nützliche Ergänzung oder praktische Erweiterung des eingesetzten IT-Systems.

Im Anhang dieser Dokumentation sind alle Verbindlichkeitsgrade jeder Anforderung kompakt in einer Tabelle zusammengefasst.

### *Anforderungsbereiche*

Auf einer dritten Strukturebene (nach Basis- und ergänzenden sowie offenen und schützenswerten Informationen) wurden schließlich die konkreten Anforderungen an Betrieb und Nutzung der IT-Systeme in der EKiR erhoben und in sechs Anforderungsbereichen zusammengestellt. Diese sind in nachstehender Grafik darstellbar:




- Die **gesetzlichen Anforderungen** umfassen rechtliche Vorgaben, die bei Nutzung und Betrieb der in der EKiR eingesetzten IT-Systeme von Relevanz sind. Hierdurch werden ein ordnungsgemeinsamer Einsatz und eine rechtssichere Nutzung von IT in der EKiR sichergestellt.

- Die **Kirchenspezifika** beinhalten religiöse und kirchenpolitische Vorgaben an Betrieb und Nutzung von IT-Systemen. Durch die explizite Berücksichtigung evangelisch-christlicher Werte und Ansichten in die IT-Standards wird der hohen gesellschaftlichen Bedeutung der Kirche Rechnung getragen.

- Die **funktionalen Anforderungen** legen fest, was das einzelne IT-System leistet. Hier werden die Erwartungen der Anwender an den Funktionsumfang des IT-Systems abgebildet.

- Die **Non-funktionalen Anforderungen** sind qualitative Anforderungen und entscheidend für die Zufriedenheit der Kunden und Anwender.

- **Sicherheitsanforderungen** schließlich dienen dem Schutz vor Gefahren und Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken.

- Die **betrieblichen Anforderungen** beschreiben die technischen Anforderungen an den Betrieb von IT-Systemen in der EKiR. Sie stellen die grundsätzliche Einsatzfähigkeit der IT-Systeme sicher. Dabei ist aus den Standards nicht abzuleiten, wer diese Betriebsleistungen

erbringt. Insbesondere Sourcing-Entscheidungen werden hiermit nicht vorweg genommen. Vielmehr gelten die betrieblichen Anforderungen allgemein für jedwede Leistungserbringer im technischen Bereich.

## *Anwendbarkeit und Relevanz der Anforderungen und Standards*

Hinsichtlich der Bedeutung und Anwendbarkeit der dokumentierten Anforderungen und der daraus hervorgehenden IT-Standards für die Nutzung und den Betrieb von IT-Systemen in der EKiR sollten folgende Aspekte bedacht werden:

- **Neuigkeitswert**
  Die weit überwiegende Anzahl der dokumentierten Anforderungen bestehen nicht erst mit der Erstellung dieser Dokumentation, sondern sind auch heute schon – teilweise auch jahrelang – existent. Insofern beinhaltet diese Dokumentation auf der inhaltlichen Ebene keine neuen Regelungen oder Festlegungen. Hier wird deskriptiv dargestellt, welche Anforderungen in welchen Verbindlichkeitsgraden heute zu beachten sind. Neu ist jedoch die kompakte und gebündelte Dokumentation der Anforderungen, die die Kenntnis und Ableitung von Handlungsbedarfen erst ermöglicht.

- **Konsequenzen**
  Mit der Übersicht der IT-Anforderungen in diesem Baukastensystem wird schnell transparent, unter welchen Bedingungen IT in der EKiR eingesetzt werden darf, soll und kann. In der Konsequenz lässt sich aus diesem Dokument z. B. ableiten, dass ein IT-System, welches nicht die Muss-Basisanforderungen erfüllt, in der EKiR nicht eingesetzt werden darf.

- **Geltungsbereich**
  Die Anforderungen gelten analog und homogen für alle kirchlichen Körperschaften von der Gemeinde bis zur Landeskirche. Sie gelten ebenso für alle Haupt- und nebenamtlich beschäftigen Personen sowie für Ehrenamtliche und alle Funktionsträger/-innen, die im Auftrag der Kirche IT nutzen und kirchliche Informationen verarbeiten.

- **Menschliches Verhalten und Technik**
  Die dokumentierten Anforderungen beziehen sich in nur geringem Maße auf den technischen Betrieb von IT. Viel bedeutsamer ist die Auswirkung auf das menschliche Verhalten sowohl der einzelnen Nutzerinnen und Nutzer als auch auf die Entscheidungsträgerinnen und –träger. Das in der heutigen Praxis wahrzunehmende Nutzungsverhalten und die Grundlagen zur Entscheidungsfindung werden durch Beachtung dieser Standards teilweise massiv beeinflusst. Dies beginnt bei Entscheidungen über Beschaffung, die Auswahl der Lieferanten, die Vorlieben für funktionale Anforderungen im Vergleich zu Sicherheits- und gesetzlichen Anforderungen, die zur Auswahl bestimmter Hersteller führen und mündet bei Sanktionen für nicht standardkonformes Verhalten in der Nutzung von IT.

- **Auswahl von IT-Lösungen**
  Die dokumentierten Anforderungen beinhalten keine Empfehlungen für die Auswahl und Nutzung konkreter IT-Systeme und IT-Lösungen. Es werden insbesondere keine standardkonformen IT-Lösungen vom Einsatz ausgeschlossen.

- **Betriebs- und Organisationsmodelle**

Durch die dokumentierten Standards werden an dieser Stelle keine organisatorischen Festlegungen getroffen. Insbesondere die funktionalen Anforderungen stellen keine Empfehlungen zur Organisation dar (Bsp.: Aus der funktionalen Anforderung, dass ein Groupware-System die Buchung von Besprechungsräumen ermöglichen soll, wird nicht definiert, dass diese Funktion EKiRweit über alle Gliederungen durchgängig erfolgen soll).

- **Kosten und Finanzierung**

  Wie bereits beschrieben, beinhalten die dokumentierten IT-Standards kaum neue Festlegungen und Anforderungen, sondern beschreiben die auch heute bestehenden Notwendigkeiten. Unter anderem aufgrund der heute ungeregelten Verantwortungen für IT, der nur punktuell vorhanden IT-Fachkonzepte und der differenzierten Betriebsmodelle kann davon ausgegangen werden, dass ein großer Teil der notwendigen Anforderungen heute nicht umgesetzt ist und mithin auch keine Kosten verursacht (abgesehen von der latenten Bedrohung bei Schadensersatz oder Imageverlust z. B. bei Datenschutzverletzungen). Es ist daher davon auszugehen, dass die Umsetzung der Anforderungen in den Organisationen der EKiR einen Mehraufwand im Vergleich zum Status Quo darstellt. Dieser kann sicher an einigen Stellen durch effizientere Betriebsmodelle kompensiert werden. Dennoch wird an vielen Stellen die Kostenfrage zu stellen sein. Die dokumentierten Anforderungen beantworten diese Frage nicht – zum einen aufgrund fehlender Relevanz an dieser Stelle, zum anderen auch mangels Vergleichbarkeit: Die heutige IT-Organisation mit Ihren Leistungen und Qualitäten (zu denen auch der eher nicht vorhandene Betrieb unter Beachtung der IT-Standards zählt), ist mit der eigentlich notwendigen IT-Organisation nicht vergleichbar. Ein Kostenvergleich würde hier nicht zielführend sein. Im Übrigen sollte bei allen Finanzierungs- und Kostenbetrachtungen auch der Nutzen der IT verglichen und bewertet werden. Schließlich sind insbesondere in der Verwaltung, aber zunehmend auch in der Seelsorge andere und eher effizientere Aufgabenerfüllungen durch den Einsatz von IT möglich. Insgesamt sollte die Kostendiskussion erst im Kontext der Organisationsausprägung erfolgen (nach Definition der grundsätzlichen Organisationsstrukturen für IT).

### *Aufbau der Anforderungsdokumentation*

Die in diesem Dokument erfassten Anforderungen an die Nutzung und den Betrieb von IT-Systemen folgt einem strukturierten und über alle Anforderungen identischen Aufbau.Dieser orientiert sich an nachstehender Übersicht:

**1.1. Name der Anforderung**

| | | |
|---|---|---|
| | | **Version n.n vom xx.yy.zzzz** |
| **Beschreibung** | **Beispiele** | |
| *allgemeine Beschreibung der Anforderung* | *Praxisbeispiel(-e), wie sie möglicherweise in der EKiR vorkommen* | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| *Aufzählung von Vorteilen und Argumenten für die Anforderung* | *Aufzählung möglicher Nachteile und Wirkungen der Anforderung* | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | *Muss/Soll/Kann* | *Muss/Soll/Kann* |

Die Dokumentation besteht auf folgenden Elementen:

- Klare **Bezeichnung** der Anforderung in der Überschrift

- **Versionskennzeichnung** einer jeden Anforderung mit Versionsnummer und Datum der letzten Änderung zur effektiveren Kenntnisnahme von Änderungen

- **Beschreibung** der Anforderung, die gerade auch Nicht-IT-Fachpersonen die Relevanz und inhaltliche Bedeutung der Anforderung näher bringen soll

- **Beispiele**, die die Bedeutung der Anforderung im Kontext der Verwendung innerhalb der EKiR verdeutlichen

- Darstellung des **Nutzens** bzw. der **Begründung** für die Auswahl und Relevanz der Anforderung

- Aufzeichnung der **Konsequenzen** (z. B. für Verhalten oder Organisation) bei Umsetzung der Anforderung sowie der **Risiken**, wenn die betreffende Anforderung nicht umgesetzt wird.

- **Verbindlichkeitsgrade** in der Differenzierung nach offenen bzw. schützenswerten Inhalten.

# 1. *Betriebliche Anforderungen*

## 1.1. *Nutzung von Standardprotokollen*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Nutzung von Standardprotokollen beschreibt das Einsetzen von Kommunikationsprotokollen für den Austausch von Informationen und Daten zwischen Endgeräten bzw. Prozessen, die in einem verteilten System miteinander verbunden sind. Standardprotolle sind im E-Mail-Verkehr (SMTP), Webseitenaufbau (HTTP, HTTPS) und Datei-Verkehr (FTP) üblich. Die Funktionen der Standardprotokolle bauen i.d.R. aufeinander auf. | | |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • sicherer und zuverlässiger Verbindungsaufbau<br>• verlässliches Zustellen von Informationen und Daten<br>• Wiederholtes Senden nicht angekommener Informationen und Daten<br>• Erreichen des gewünschten Empfängers/der gewünschten Empfängerin<br>• Sicherstellen einer fehlerfreien Übertragung<br>• Richtige Reihenfolge der Daten und Informationen<br>• Verhindern von Diebstahl und Manipulation | | • Verlust der IT Sicherheit<br>• Kompatibilität der Protokolle mit den IT Systemen<br>• geschulter IT Support |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 1.2. *Skills/ Wissen bei IT Personal*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Das Skill- und Wissensniveau des EKiR IT Personals beschreibt die Tiefe und Breite der Fähigkeiten der IT Mitarbeiter/-innen in Bezug auf die Groupware in den Punkten Administration und Anwenderbetreuung. Ein kompetentes Auftreten gegenüber den Nutzenden ermöglicht eine höhere Akzeptanz und Nutzungsbereitschaft. Wichtig dabei ist ebenfalls die Art und Weise, wie der Transfer an die Nutzenden stattfindet. | | • Mitarbeiter/-in im IT Service ist auskunftsfähig zum vollen Funktionsumfang der Groupwarelösung oder des Mewis NT |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Kompetente Ansprechpartner/-innen für die Groupwarenutzenden<br>• Schnelle und unkomplizierte Anwenderhilfe<br>• effizientes Incident- und Problemmanagement<br>• Know-how Transfer für die Nutzenden | | • erhöhter Schulungsaufwand<br>• höherer Aufwand bei der Mitarbeitergewinnung<br>• Qualifiziertes / ausgebildetes IT-Fachpersonal (z. B. Fachinformatiker/innen)<br>• ggf. Sourcing-Modelle (Interne Bündelung, Outsourcing)<br>• ggf. höhere Kosten bei der Mitarbeitergewinnung<br>• ggf. höhere Gehaltskosten aufgrund größerer Aufgabenbereiche |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 1.3. *On-/Offboarding*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Onboarding beschreibt das Einstellen bzw. Integrieren eines/r neuen Mitarbeiters/-in in die EKiR. Dieser Einarbeitungsprozess ist beidseitig organisiert. Bezogen auf die Groupware beschreibt das Onboarding eine Lernkurve im Umgang von der Unwissenheit in der Nutzung bis zum erfolgreichen Wissenstransfer.<br><br>Offboarding ist das Gegenstück; nämlich der Trennungsprozess. Im Sinne der Definition ist dieser Prozess bewusst gestaltet inkl. der Sicherstellung von Deaktivierung und Dokumentation der Zugangsberechtigung eines/r ausgeschiedenen Mitarbeiters/-in, um Datenmissbrauch und Diebstahl zu verhindern. Es muss beschrieben werden, wie mit den Daten und Zugriffsrechten im Falle des Ausscheidens zu verfahren ist.<br><br>Im Falle eines Ausscheidens eines Mitarbeitenden ist sicherzustellen, dass sämtliche Zugriffsrechte auf Daten und Informationen deaktiviert und nach einem festgelegten Zeitraum zu löschen sind. Zwischen Deaktivierung und Löschung muss sichergestellt sein, dass bspw. eingehende E-Mails gesichtet und ggf. weiterbearbeitet werden. | • Benutzerprofilanlegung eines/r Mitarbeiters/-in in der EKiR an einer zentralen Stelle , Zuordnung weiterer Gruppenzugehörigkeiten, dezentral auf KKR-Ebene<br><br>• Deaktivierung und spätere Löschung des Benutzerprofils eines/-r nicht mehr wiedergewählten Presbyters/-in |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |

| | |
|---|---|
| • Positive Wahrnehmung der EKIR als Arbeitgeber<br>• Sicherheitsgewährleistung<br>• Sicheres Handling der Groupware<br>• Mitarbeiterbindung und Identifikation | • Höhere Einarbeitungskosten<br>• Überforderung neuer Nutzenden<br>• Sicherheitslücken beim Ausscheiden von Mitarbeitenden oder Anwendern/-innen |

| | offene Inhalte | vertrauliche/schützenswerte Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Muss | Muss |

## 1.4. *Wirtschaftlichkeit im Betrieb*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Wirtschaftlichkeit im Betrieb ist das Maß für das effiziente Kosten-Nutzen-Verhältnis einer eingesetzten Groupwarelösung. Dabei wird verglichen, in welchem Verhältnis der benötigte Mitteleinsatz (Technische Infrastruktur, Hard- und Software, Mitarbeiterschulung, Support) und der erreichte Erfolgs steht.<br><br>Um dieses Verhältnis messen zu können, müssen erfolgskritische Faktoren festgelegt werden, bspw. Antwortgeschwindigkeit auf E-Mail Eingang in der Seelsorge oder Schnelligkeit in der Terminfindung für eine Presbytersitzung. | | • Open Source vs. proprietäre Groupwarelösung<br>• Basis-Groupwarelösungen mit Grundfunktionen (E-Mail, Kalender, Adressbuch) vs. Enterprise-Lösungen mit vollem Funktionsumfang<br>• Webclients vs. Desktopclients |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Sicherstellen, dass Kosten und Nutzen einer Groupwarelösung mit den wirtschaftlichen Grundsätzen der EKIR in Einklang stehen<br>• Positive Auswirkung im Sinne einer Vorbildfunktion<br>• Herstellersupport bei proprietärer Software<br>• Kostenersparnis bei Open Source Lösung | | • Transparente Kostenstruktur<br>• Einheitliche Leistungskennzahlen (KPIs)<br>• Einheitliche kritische Erfolgsfaktoren (KEFs)<br>• Höherer finanzieller Administrationsaufwand und damit Verwaltungskosten<br>• Steuerungsaufwand |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 1.5. *Schnittstellen/ Datenaustausch bei verteilten Betriebsstandorten*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Schnittstellen und Datenaustausch beschreibt die Übertragung von Daten und Informationen bei der Kommunikation zwischen zwei oder mehreren Standorten der EKIR, bspw. dem Landeskirchenamt in Düsseldorf und den Standorten der 38 Kirchenkreise und/oder 739 Gemeinden. Hierbei werden sowohl offene als auch vertrauliche/schützenswerte Inhalte verschickt. | | • Das Landeskirchenamt möchte allen Gemeinden Zugriff auf ein Diskussionspapier zur Veränderung der Kirchenordnung geben. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Zusammenarbeit zwischen den Verwaltungseinheiten der EKIR<br>• Kosteneinsparung | | • Höhere Anforderungen an Administration und Support<br>• Vereinheitlichung der IT Infrastruktur unter den Gesichtspunkten der Datenkompatibilität<br>• Schnittstellenproblematik (siehe Bespiel NKF) |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Muss |

## 1.6. *API-Schnittstellen*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| API Schnittstellen sind Programmierschnittstellen, die es ermöglichen, über die Groupware Zugriff auf andere Programme und umgekehrt zu gewähren. So ermöglicht bspw. eine API zum Dokumentenmanagementsystem einen Aufruf einer Datei als Anhang für eine E-Mail oder es können Kontaktdaten aus der entsprechenden Groupwarefunktion automatisch an das Meldewesen weitergegeben werden. Aus IT-Sicherheitsgründen ist der Anbindung an mobile Endgeräte besondere Aufmerksamkeit zu widmen. | | • Abgleich von Kontaktinformationen von Gemeindemitgliedern zwischen Mewis NT und Groupwarelösung |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Verlustfreier Austausch von Daten zwischen den Anwendungen<br>• Authentizität der verwendeten Daten<br>• Beschleunigung der Tätigkeitsabläufe<br>• Integration verschiedener Systeme, ohne dass eine kostenintensive Gesamtlösung beschafft werden muss | | • Höherer Anforderungsbedarf an die verwendete Software<br>• Kompatibilität zwischen den Systemen und Daten<br>• Höherer Support und Administrationsaufwand |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Kann |

## 1.7. *Datenübernahme von anderen Systemen (Kompatibilität)*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Groupware ist in der Lage, Daten aus allen notwendigen in der EKiR verwendeten IT Programmen zu lesen bzw. zu verarbeiten. Die Datenübernahme beschreibt die Verarbeitungs- oder Lesefunktion der Groupwarelösung von Informationen und Daten aus Fremdsystemen. Das betrifft auch die Übernahme von Daten aus Alt- oder Vorgängersystemen der Groupware. | | Daten und Informationen aus anderen bei der EKiR eingesetzten Systemen können ohne Einschränkung oder Migration von der Groupwarelösung verarbeitet werden |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Beschleunigung der Tätigkeitsabläufe<br>• Keine Vereinheitlichung der Systemlandschaft nötig; damit möglicherweise Kostenersparnis<br>• Flexibilität | | • Höherer Anforderungsbedarf an die verwendete Software<br>• Kompatibilität zwischen den Systemen und Daten<br>• Höherer Support und Administrationsaufwand<br>• Höhere Anforderung an Datensicherheit<br>• Standardisierte Verhaltensregel für Umgang und Benutzung von Fremdsystemen |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Kann |

## 2. *Gesetzliche Anforderungen*

### 2.1. *Anforderungsprofil und Programmdokumentation*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Für alle in der EKiR eingesetzten E-Mail- und Groupware-Softwarelösungen werden im Vorfeld Anforderungsprofile erstellt. In diesen Anforderungsprofilen werden die gewünschten Funktionen beschrieben. Zudem liegt für jede Softwarelösung eine Programmdokumentation mit Informationen über:<br>• die Installation,<br>• den Betrieb und<br>• die eingesetzten Funktionen<br>vor. | | Vor dem Einsatz der Outlook-E-Mail-Software wird genau geprüft, welche Funktionen mit dieser Software möglich sein sollen (z.B. E-Mail-Weiterleitung, Import und Export des Adressbuches, automatische Transport-verschlüsselung).<br><br>Da die Mitarbeitende neu im Sekretariat angefangen hat, ist sie noch nicht mit dem Umgang des E-Mail-Programmes vertraut. Eine vorliegende Programmdokumentation hilft Ihr bei der Einarbeitung in das Programm. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Das Anforderungsprofil hilft kirchlichen Stellen, sich für das richtige, angemessene Produkt zu entscheiden.<br><br>Fehlentscheidungen werden minimiert und eine Wirtschaft-lichkeit der eingesetzten Produkte gefördert.<br><br>Es liegt eine klare Entscheidungsgrundlage dokumentiert vor, die bei der Auswahl des passenden Produktes hilft. | | Vor Beschaffung und Einsatz entsteht Aufwand, der bisher nicht vorgesehen war.<br><br>Technische Voraussetzungen Client definieren. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.2. *Gewährleistung der IT-Sicherheit*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Jede kirchliche Stelle und somit alle Mitarbeitenden verpflichten sich, IT-Sicherheit zu gewährleisten. Durch die Umsetzung des Sicherheitskonzeptes sorgt die Kirche für IT-Sicherheit. Dies bedeutet, dass alle Mitarbeitenden in das Sicherheitskonzept eingebunden sind und damit verpflichtet sind, Maßnahmen für sichere E-Mail und Groupware, die im Sicherheitskonzept gefordert werden, auch angemessen umzusetzen. | | Im IT- Sicherheitskonzept wird gefordert, dass<br>• bei der Benutzung von E-Mail ein Virenscanner auf dem Computer aktiv ist,<br>• E-Mails mit vertraulichem Inhalt nur verschlüsselt versendet werden. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Wenn alle Mitarbeitenden an der Umsetzung des Sicherheitskonzepts beteiligt werden, dann wird das Risiko extrem minimiert, dass<br>• vertrauliche Informationen ungewollt veröffentlicht werden<br>• die Verfügbarkeit durch Virenangriffe beeinträchtigt wird<br>• Integritätsverluste (fehlerhafte Datenverarbeitung) auftreten | | Mitarbeitende müssen bezüglich Sicherheitsanforderungen Informiert bzw. geschult werden. Diese Schulungen sind am Markt erhältlich.<br><br>Mitarbeiter müssen (vertraglich) auf Einhaltung der Sicherheitsanforderungen verpflichtet werden<br><br>Jede kirchliche Stelle hat ein IT-Sicherheitskonzept zu erstellen. Es sei denn, mehrere kirchliche Stellen arbeiten in einem IT-Verbund, dann ist das Konzept für den IT-Verbund zu erstellen. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.3. *Gewährleistung des Datenschutzes*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | | **Beispiele** |
| Mitarbeitende müssen bei der E-Mail und Groupware-Nutzung die Anforderungen des EKD-Datenschutzgesetzes einhalten. Dazu zählt der gewissenhafte Umgang mit schützenswerten personenbezogenen Daten. Zudem wird ein Datenschutzbeauftragter ernannt, der bei Unklarheiten oder sonstigen Fragen als Ansprechpartner dient. | | Ein Pfarrer der Gemeinde möchte außerplanmäßig sämtliche Gemeindeglieder über eine plötzliche schwere Krankheit eines bekannten Gemeindemitgliedes informieren. Ist er ausreichend über die persönlichen Datenschutz Anforderungen informiert? |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Die Gewährleistung des Datenschutzes in der Kirche ist ein Recht aller Beteiligten. Eventuelle entstehende Schadenersatzforderungen aufgrund einer Verletzung könnten minimiert werden. | | Es muss für jede datenschutzrechtlich relevante kirchliche Einrichtung und Organisation einen verantwortlichen Datenschutzbeauftragten geben.<br><br>Ein Datenschutzbeauftragter kann auch für viele Bereiche zuständig sein. Dies muss explizit geregelt und den Mitarbeitenden bekannt gemacht werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.4. *Gewährleistung Lizenzsicherheit*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | | **Beispiele** |
| Alle eingesetzten Softwareprodukte müssen mit einer gültigen Softwarelizenz ausgestattet sein. Zudem ist bei der Planung eine ausreichend lange Gültigkeit im Anforderungsprofil (siehe Anforderungsprofil und Programmdokumentation) festzulegen bzw. die Gültigkeit der Softwarelizenz ist regelmäßig zu prüfen. | | Zur automatisierten Versendung eines Newsletters per E-Mail nutzt die Gemeinde XY eine lizenzpflichtige Software, die sie beim Hersteller käuflich erworben hat. Die Nachbargemeinde hat sich diese Software kopiert und nutzt diese mit dem gleichen Lizenzschlüssel. Nach einem Jahr meldet sich der Hersteller und verlangt die Nachzahlung der Lizenzgebühr und eine zusätzliche Strafgebühr. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Wenn Sie sich um die ordnungsgemäße Sicherstellung von Softwarelizenzen kümmern, dann können Strafzahlungen vermieden werden.<br><br>Zudem können durch ein geschicktes Lizenzmanagement der EKiR die Kosten der eingesetzten Software massiv gesenkt werden. | | Die Gewährleistung von Lizenzsicherheit bedeutet auch, dass die eingesetzte Software geprüft werden muss. Zudem müssen in die Konzeption bereits dementsprechende Prüfungen aufgenommen werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.5. *Test der Anwendung*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Anwendungen müssen vor dem produktiven Einsatz einem Test unterzogen werden. Ein solcher Test enthält mindestens die folgenden Aspekte:<br>• Eingangsprüfungen (Prüfung auf Computer-Viren, Lauffähigkeit in der gewünschten IT-Einsatzumgebung, ....),<br>• funktionale Tests (Überprüfung der funktionalen Anforderungen),<br>• Tests weiterer funktionaler Eigenschaften (Überprüfung von Kompatibilität, Performance, Interoperabilität, Konformität mit Regelungen oder Gesetzen, Benutzerfreundlichkeit, Wartbarkeit, Dokumentation),<br>• sicherheitsspezifische Tests (Überprüfung der Sicherheitsanforderungen) und<br>• Pilotanwendungen können wertvolle Informationen im Rahmen des Tests geben. | | Ein Testplan kann diese Inhalte haben:<br>• Festlegung der Testinhalte anhand des Anforderungskataloges,<br>• Überprüfung von Referenzen,<br>• Festlegung des Gesamtprüfaufwandes,<br>• Zeitplanung einschließlich Prüfaufwand je Testinhalt,<br>• Festlegung der Testverantwortlichen,<br>• Testumgebung,<br>• Inhalt der Testdokumentation,<br>• Festlegung von Entscheidungskriterien. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Durch das Testen der Anwendung wird ein ordnungsgemäßer und sicherer Betrieb des E-Mail oder Groupware-Systems sichergestellt. | | Um einen solchen Test zu konzipieren, sollte das Anforderungsprofil im Vorfeld erarbeitet worden sein.<br>Tests von Groupware-Lösungen führen zu erhöhtem Aufwand und zu einer Verzögerung zwischen Planung, Entscheidung und Einsatz einer Software-Lösung. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.6. *Wirtschaftlichkeit*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | **Beispiele** | |
| Bei der Beschaffung von E-Mail- und Groupware-Systemen sind Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten und im Anforderungsprofil zu berücksichtigen. | Vor einer Beschaffung muss im Anforderungsprofil auch die Wirtschaftlichkeit als Anforderung geprüft werden.<br><br>Es gibt neben kostenpflichtiger E-Mail-Software (z.B. Microsoft Outlook) auch kostenlose Open Source-Software, wie z.B. Mozilla Thunderbird oder Outlook Express. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| Durch Wirtschaftlichkeit und Sparsamkeit wird Nachhaltigkeit gefördert. | Es kann vorkommen, dass eine günstigere Lösung von einem bereits großflächig eingesetzten Produkt eingesetzt wird. In diesem Fall müssen eventuelle Inkompatibilitäten und erhöhte Einarbeitungszeit der Mitarbeitenden mit einbezogen werden. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.7. *Berücksichtigung der BSI Anforderungen*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Das Bundesamt für Sicherheit in der Informationstechnologie gibt in den IT-Grundschutzkatalogen organisatorische und technische Maßnahmen vor, die für einen sicheren Betrieb von E-Mail und Groupware notwendig sind. Die EKiR berücksichtigt diese Maßnahmen und setzt diese unter Maßgabe der Wirtschaftlichkeit und Kirchenspezifika sinnvoll um. | | Für den Einsatz von E-Mail macht das BSI Vorgaben zur Schulung bzw. Einweisung von Mitarbeitenden für die sichere Nutzung von E-Mail-Clients. Der Nutzer wird auf die ihn betreffenden Regelungen, z.B. das Verbot zum massenhaften weitersenden von Kettenbriefen hingewiesen.<br><br>Für den Einsatz von E-Mail macht das BSI Vorgaben zur sicheren Konfiguration der Software. Bei der Installation informiert sich der entsprechende Mitarbeitende über die Anforderungen der EKiR und der IT-Grundschutzkataloge (B 5 Anwendungen -> Groupware), ob alle Maßnahmen beachtet werden. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Das Berücksichtigen der BSI-Anforderungen hilft den kirchlichen Stellen, mögliche Sicherheitsprobleme im Vorfeld zu minimieren.<br><br>Die IT-Grundschutzkataloge stellen Maßnahmen zur Verfügung, die auf organisatorischer und technischer Ebene Hilfestellungen geben. | | Bei der Umsetzung der Maßnahmen muss immer auch der Aspekt der Wirtschaftlichkeit geprüft werden. Erfolgt dies nicht, so können aufgrund der Menge der Maßnahmen wichtige Umsetzungen verzögert oder gar verworfen werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.8. *Erstellung Sicherheitskonzept*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Ein Informationssicherheitskonzept beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele der EKiR zu erreichen. Das Sicherheitskonzept (SIKO) ist das zentrale Dokument im Sicherheitsprozess der EKiR und gilt jeweils für einen speziell definierten Informationsverbund. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Aus diesem Grund muss ein Sicherheitskonzept sorgfältig geplant und umgesetzt, sowie regelmäßig überprüft werden.<br><br>Unter einem Informationsverbund (oder auch IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.<br><br>Komplexe Aufgabenbereiche oder Fach-Anwendungen können in eigenen Sicherheitskonzepten behandelt werden.<br>In einem Sicherheitskonzept für E-Mail und Groupware wird der betrachtete Bereich klar eingegrenzt. Alle im Bereich wesentlichen Objekte (Infrastruktur, IT-Systeme, Netze und Anwendungen) werden mit der Strukturanalyse erfasst. Weitere | Das Sicherheitskonzept der EKiR ist ein Dokument, in dem allgemeine Vorgehensweisen und Maßnahmen, die gesamte EKiR betreffend beschrieben werden. Das wäre z.B. die Sicherheitsmaßnahme, dass jede neue Softwarelösung in die Sicherheitskonzeption aufzunehmen ist.<br><br>Im Bereich Personal werden spezifische IT-Lösungen eingesetzt, z.B. eine Datenbank, in der alle Mitarbeitenden-Daten erfasst sind und eine Software zur Abrechnung der Gehälter. Für die Abteilung Personalwesen wird ein Sicherheitskonzept „SIKO-Personalwesen“ erstellt, welches nur den Bereich Personal betrachtet, z.B. die besondere Absicherung der Personaldatenbank.<br><br>Standardmäßig hat jede kirchliche Stelle einen eigenen Informationsverbund zu definieren und dafür ein Sicherheitskonzept zu erarbeiten. Es kann aber auch sein, dass eine kirchliche Stelle zu einem größeren Informationsverbund gehört (angeschlossen ist), so dass dort das Sicherheitskonzept der übergeordneten Instanz gilt. |

| | |
|---|---|
| Schritte der Vorgehensweise werden im BSI Standard 100-2 vorgestellt. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Eine Sicherheitskonzeption hilft der EKiR dabei, sich einen aktuellen Überblick über mögliche Gefährdungen Ihrer Informationen und Systeme zu verschaffen und angemessen darauf zu reagieren.<br><br>Eine Sicherheitskonzeption minimiert die Risiken bezüglich schwerwiegender Notfälle, bedingt durch fehlerhafte Datenverarbeitung, wie z.B. Enthüllung kirchlicher Daten oder Mitgliederinformationen, sowie die längerfristige Verhinderung von kirchlichen Aufgaben (Telefonseelsorge, Finanzverwaltung, Mitgliederinformierung, etc). | Das erstmalige Erstellen eines Sicherheitskonzeptes bedeutet einen erhöhten Aufwand für die Bereiche der EKiR. Deshalb ist eine professionelle Planung vor Beginn notwendig, da sonst eine angemessene Umsetzung dieser Anforderung nicht gewährleistet ist.<br><br>Alle Bereiche der EKiR müssen in diesen Prozess mit einbezogen werden.<br><br>Ausgewählte Mitarbeitende aller Bereiche der EKiR müssen bezüglich der Erstellung einer Sicherheitskonzeption geschult werden. Diese Schulungen sind am Markt erhältlich. |

| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
|---|---|---|
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.9. *Gewährleistung rechtssichere Archivierung*

| | **Version 0.9 vom 04.06.2013** |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die rechtssichere Archivierung von archivwürdigen Dokumenten, die durch E-Mail- und Groupware-Nutzung entstehen, ist entsprechend den bei der EKiR existierenden Vorgaben zur daten-schutzkonformen und rechtssicheren Archivierung vorzunehmen und verbindlich festzulegen. Dazu gehören Auf-bewahrungs- und Kassations- | Ein Pfarrer möchte seine wichtigen E-Mails und Kontaktinformationen im Rahmen seiner Seelsorgearbeit archivieren und informiert sich über rechtssichere Archivierung im Archivierungskonzept. Das liefert ihm wichtige Vorgaben zur Archivierung von E-Mails. |

| | |
|---|---|
| ordnung sowie Schriftgutordnung (SGO). All diese Vorgaben müssen im Archivierungskonzept für E-Mail und Groupware aufgenommen werden. Dies betrifft unter anderem:<br><br>• Mindestaufbewahrung aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen,<br>• Höchstaufbewahrungsdauer aus Datenschutzgründen,<br>• Zugriffsrechte für externe Stellen sowie<br>• Qualität von digitalen Signaturen.<br>• Beachtung Kassationsordnung / Archivordnung und ggf. weiterer Verordnungen und Gesetze.<br><br>Weitere Informationen siehe BSI Grundschutzkataloge M 2.243 Entwicklung des Archivierungskonzepts. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Es gibt gesetzliche Vorschriften zur Archivierung, die bei Nichteinhaltung unter Umständen zu Strafzahlungen oder anderen Ansprüchen gegenüber Dritten führen. | Ein Archivierungskonzept muss ausgearbeitet werden, das die spezifischen Aspekte der zu archivierenden Daten und E-Mails und Groupware beinhaltet. |

| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.10. *Verhaltensregeln bei Verdacht auf Sicherheitsvorfall*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Als Sicherheitsvorfall wird ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die IT-Sicherheit hat und in der Folge große Schäden nach sich ziehen kann. Typische Folgen von Sicherheitsvorfällen können die Ausspähung, Manipulation oder Zerstörung von Daten sein. Um Schäden zu vermeiden bzw. zu begrenzen, müssen Sicherheitsvorfälle schnell und effizient bearbeitet werden.<br>Dazu müssen die folgenden Anforderungen umgesetzt werden:<br>• Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen<br>• Festlegung von Meldewegen für Sicherheitsvorfälle<br>• Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen<br>• Erkennen und Erfassen von Sicherheitsvorfällen<br>• Hinzuziehen von internen und externen Experten<br>• Eindämmen der Auswirkung von Sicherheitsvorfällen<br>• Nachbereitung von Sicherheitsvorfällen<br>• Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen<br>• Dokumentation von Sicherheitsvorfällen | Typische Sicherheitsvorfälle sind beispielsweise:<br>• Fehlkonfigurationen, die zur Offenlegung vertraulicher Daten, zum Verlust der Integrität schutzbedürftiger Daten oder zu Datenverlusten führen,<br>• Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten,<br>• Auftreten von Schadsoftware oder<br>• kriminelle Handlungen (etwa Hacken von Internet-Servern, Einbruch in IT-Systeme, Diebstahl von Daten, Sabotage oder Erpressung mit IT-Bezug).<br>Ein Beispiel für Schadsoftware ist folgender Sicherheitsvorfall:<br>• Es treten zunächst sporadisch, dann massenhaft neue Computer-Viren mit Schadfunktionen auf. Erfolgt keine rechtzeitige Reaktion, können unter Umständen ganze Organisationseinheiten arbeitsunfähig werden. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Wird auf akute Sicherheitsvorfälle angemessen reagiert, so können | Der Aufwand zur Erstellung und Umsetzung eines solchen Konzepts zur |

| | | |
|---|---|---|
| unter Umständen große Schäden bis hin zu Katastrophen verhindert werden. | Sicherheitsvorfallbehandlung ist nicht gering. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.11. *Verschlüsselung schützenswerter Daten*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die zunehmende Bedeutung von E-Mail erfordert den Einsatz von Maßnahmen, die eine Vertraulichkeit und Verbindlichkeit gewährleisten. Dies wird durch den Einsatz von Produkten zur Verschlüsselung und digitalen Signatur von E-Mails erreicht. | | Die Kirchenverwaltung sendet Mitgliederverzeichnisse per E-Mail an die Kirchengemeinde, da diese dringend benötigt werden. Die Kirchenverwaltung muss sich bewusst sein, dass sie diese Daten nur verschlüsselt übertragen darf. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Bei sensiblen personenbezogenen Daten darf eine elektronische Übermittlung über das Internet nicht unverschlüsselt stattfinden, da sonst Schadenersatzanforderungen im Falle einer Enthüllung dieser Daten an die EKiR gestellt werden könnten (siehe EKD-DSG unter § 8 Schadenersatz durch kirchliche Stellen). | | Die aktuellen Arbeitsplätze und die eingesetzten E-Mail-Systeme müssen technisch eine Verschlüsselung ermöglichen. Zudem muss der/die Empfänger/-in in der Lage sein, die E-Mail wieder zu entschlüsseln.<br><br>Alle Mitarbeitenden müssen sensibilisiert werden, dass sie die verschlüsselte Übertragung schützenswerter Informationen angemessen durchführen.<br><br>Die Betriebssicherheit einer dezentralen Lösung (ohne PKI) ist kritisch zu hinterfragen. (Backup und Restore von Daten). |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Muss |

## 3. *Kirchenspezifika*

### 3.1. *Anerkennung des EKD-DSG*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Das kirchliche Datenschutzgesetz (EKD-DSG) ist für E-Mail und Groupware anzuwenden. Das EKD-DSG sorgt dafür, dass jeder Einzelne davor geschützt wird, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Im Bereich E-Mail und Groupware kommt es zu einer automatisierten Verarbeitung von personenbezogenen Informationen. Die automatisierte Verarbeitung bezeichnet die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. | | Die Mitarbeiterin im Personalwesen des LKA ist besonders angehalten, personenbezogene Daten gemäß dem EKD-DSG zu verarbeiten. Beispielsweise dürfen Datensätze aus der Personaldatenbank nicht zweckentfremdet benutzt oder Unberechtigten zugänglich gemacht werden. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Fügt eine kirchliche Stelle der betroffenen Person durch eine nach den Vorschriften dieses Kirchengesetzes oder nach anderen kirchlichen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung ihrer personenbezogenen Daten einen Schaden zu, ist sie der betroffenen Person zum Ersatz des daraus entstehenden Schadens verpflichtet. | | Es müssen alle Mitarbeitenden auf die Datenschutzregeln verpflichtet werden. Zudem sollte jede/-r Mitarbeitende über Inhalte des EKD-DSG informiert werden (mindestens ein Merkblatt der für ihn/sie wichtigen Datenschutzanforderungen).<br><br>Wenn das Groupwaresystem bei einem Dienstleister betrieben wird, muss dieser die Einhaltung des EKD-DSG bestätigen und ein „ADV“ Vertrag zur Auftragsdatenverarbeitung muss geschlossen werden |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 3.2. *Wirtschaftsethische Fragestellungen*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Evangelische Kirche im Rheinland verpflichtet sich dem Konziliaren Prozess für Frieden, Gerechtigkeit und Bewahrung der Schöpfung. Verantwortung für die Schöpfung und soziale Gerechtigkeit sind deshalb auch bei der Beschaffung und beim Betrieb von IT wesentliche Kriterien. In der von der Landessynode der EKiR beschlossenen Handreichung „Wirtschaften für das Leben“ heißt es: „Kriterien der Nachhaltigkeit und der Gerechtigkeit sind beim Einkauf von entsprechenden Konsumwaren zu berücksichtigen (vom fair gehandelten Kaffee und Recycling-Papier über den „grünen Computer“ bis zu Baumaterialien) (Wirtschaften für das Leben 2008, S. …). | | Der „Leitfaden zum ökofairen Einkauf, der gemeinsam von der EKiR und von SÜDWIND im Mai 2010 veröffentlicht wurde, formuliert: „Um Rohstoffe für die Produkte des täglichen Bedarfs zu gewinnen, werden große Mengen Erde, Steine oder Wasser bewegt. Ein Computer mit Tastatur, Maus, Monitor und Drucker wiegt beispielsweise zwischen 6 und 10 kg. Das Gewicht aller Materialien, die für die Herstellung verwendet wurden, liegt jedoch nach Schätzungen von „Zukunft einkaufen“ bei 600 bis 1.500 kg .Dieser sogenannte „ökologische Rucksack“ beträgt demnach ein Vielfaches des eigenen Gewichts."(Effizient wirtschaften, aber kein Sparen an der falschen Stelle! Leitfaden zum ökofairen Einkauf Mai 2010, S …) |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Erfüllung des Konziliaren Prozess<br>• Bewahrung der Schöpfung<br>• Schutz von Nachhaltigkeit und Gerechtigkeit | | • Nicht Berücksichtigung von Nachhaltigkeit<br>• Reduktion von Papier<br>• Grüner Betrieb der Infrastruktur<br>• "Grüne E-Mail" 4.6 |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 3.3. *Eigenerklärung*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Eigenerklärung beschreibt das Verständnis der EKiR, eingenommene Steuern für ihre vielfältigen, in die Gesellschaft hineinreichenden Aufgaben, zu finanzieren. Darüber hinaus verpflichtet sie sich, Sozialstandards einzuhalten und unter Berücksichtigung sozialer Kriterien (§ 18 TVgG-NRW) zu wahren. | | • nur Beauftragung von Auftragnehmern, die sich bei Angebotsabgabe schriftlich verpflichtet haben, Sozialstandards einzuhalten, u.a. Kernarbeitsnormen gemäß der Internationalen Arbeitsorganisation (ILO) |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • soziale Verantwortung als Körperschaft des öffentlichen Rechts<br>• sichere, planbare und leistungsfähigkeitsbezogene Finanzierung des kirchlichen Auftrags (Verkündigung des Evangeliums in Wort und Tat)<br>• nachhaltiges Wirtschaften<br>• positive Aussenwahrnehmung der EKiR | | • Transparenz in der Steuermittelverteilung auf Personal-, Sachkosten, Verwaltung, Kirchenbauten, Schule, Bildung, Soziales und Karitatives etc.<br>• Konsequente Überprüfung der Vertragspartner und Lieferanten<br>• Erhöhte Komplexität des Vergabeverfahrens |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 3.4. *Verpflichtung Scientology*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | | **Beispiele** |
| Die Verpflichtung Scientology beschreibt die verbindliche Position der EKiR und ihrer Einrichtungen, nicht mit Scientology oder ihnen nahestehenden Organisationen und Unternehmen zusammenzuarbeiten.<br><br>Es handelt sich beim Umgang mit offenen Inhalten hinsichtlich der Verbindlichkeit um eine Soll-Anforderung. | | • Onlineangebot im Bereich Nachhilfe für leistungsschwache Schüler |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Schutz von Kindern und Jugendlichen<br>• Verhinderung von Indoktrinierung durch Sekteninhalte | | • Konsequente Durchsetzung der Verpflichtungserklärung gegenüber Unternehmen, Organisationen und deren Mitgliedern |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 3.5. *Frieden und Gerechtigkeit*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| IT-Produkte, Komponenten und Dienstleistungen dürfen nur bei Unternehmen und in Ländern beschafft oder beauftragt werden, die dem konziliaren Prozess folgend für Gerechtigkeit und Frieden eintreten. Es bedeutet, dass Unternehmen und Länder, die mit der EKiR zusammenarbeiten, nicht gegen Arbeits- und Menschenrechte verstoßen, Kinderarbeit ausschließen, nicht an der Produktion von Pornografie, Rauschgiften und Waffen jedweder Art beteiligt sind. | | • Kein Einkauf von IT Produkten oder Dienstleistungen von Unternehmen aus China aufgrund unsicherer Menschenrechtslage und unzureichender Arbeitsbedingungen in den Produktionsbetrieben |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Klare Position der EKiR in den Punkten Friedenswahrung und Gerechtigkeit<br>• Berücksichtigung von ethischen und sozialen Aspekten bei der Beschaffung<br>• direkter Bezug auf kirchliche Werte und Texte | | • konsequente Überprüfung von Produzenten, Anbietern und Lieferanten von IT Produkten, Komponenten und Dienstleistungen<br>• keine Beauftragung bei Verstößen gegen Arbeits- und Menschenrechte, Diskriminierung, Kinderarbeit, Korruption, Geldwäsche |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 3.6. *Bewahrung der Schöpfung*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Bewahrung der Schöpfung bezeichnet die ressourcenschonende Verwendung von Energie und Einsatzmaterialen in der Informations- und Kommunikationstechnologie sowie einen Ausschluss der Zusammenarbeit mit Unternehmen, die mit ihren Geschäftszielen und Produkten die Natur bewusst verändern und/oder schädigen. D.h. dass bereits bei der Entwicklung nicht nur ein möglichst ressourcenschonender Umgang der Technik im Betrieb, sondern auch eine umweltschonende Entsorgung und Wiederverwendung der Einsatzmaterialien Berücksichtigung findet. | • Versorgung des Rechenzentrums mit Strom aus erneuerbaren Energiequellen<br>• Einsparung von Papier- und Druckmaterialen durch die Orientierung am Prinzip des papierlosen Büros<br>• Strombezug aus erneuerbaren Energien<br>• Einhaltung § 17 TVgG-NRW |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Schonung von Energie und Rohstoffressourcen<br>• Positive PR für die EKiR<br>• Einsparung von Kosten hinsichtlich Verbrauchsgüter wie bspw. Papier, Toner etc.<br>• Klare und konsequente Positionierung der EKiR in den Punkten Umweltschutz, Gentechnik, Atomenergie und Tierversuche | • Standardisiertes Verhalten aller Mitarbeiter<br>• Genaue Prüfung der Bezugsquellen von Stromlieferanten<br>• Mögliche Kostensteigerung beim Strombezug<br>• Keine Beauftragung von Unternehmen aus den Bereichen „grüner“ Gentechnik, spezialisierten Unternehmen im Bereich Embryonen-Forschung, Atomenergie, Tierversuche<br>• Ausschluss der Zusammenarbeit mit Unternehmen, für die eine massive Verletzung von Umweltgesetzen nachgewiesen ist bzw. die allgemein anerkannte ökologische Mindeststandards und Verhaltensregeln missachten<br>• Keine Outsourcingaufträge in Länder vergeben, die das Kyoto Protokoll nicht ratifiziert haben und die Todesstrafe nicht abgeschafft haben. |
| **offene Inhalte** | **vertrauliche/schützenswerte** |

| | | Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Soll |

## 3.7. *Wiederverwendbarkeit landeskirchlich-übergreifender Lösungen*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Wiederverwendbarkeit landeskirchlich-übergreifender Lösungen beschreibt den Einsatz von bewährten und standardkonformen IT Lösungen in der gesamten EKiR von der Gemeinde bis zur Landeskirche. | • Einführung einer EKiR-weit genutzten Groupwarelösung | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Einhaltung von IT Standards<br>• Kostenersparnis<br>• Nutzeneffekte<br>• Sicherheitsgewinn<br>• Steigerung von Effizienz und Effektivität | • Zentrale IT Steuerung<br>• Schulung der Nutzenden<br>• Gewährleistung eines übergreifenden Supports | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 3.8. *Nachhaltigkeitsnachweis*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | | **Beispiele** |
| Jedes IT Produkt besitzt einen Lebenszyklus, beginnend in der Planungs- oder Beschaffungsphase über Do- bzw. Installationsphase bis zur Check- oder Betriebsphase. Der Nachhaltigkeitsnachweis beschreibt die Sicherstellung, dass unnötige Kosten sowie kalkulierbare und nicht kalkulierbare Risiken minimiert sind. | | • Einhaltung § 17 TVgG-NRW |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Kostensenkung<br>• Verkürzung von Lieferzeiten<br>• Schnellere Inbetriebnahme von IT-Systemen<br>• Langlebigkeit des Produkts bei sichergestellter Leistungsfähigkeit | | • Pflege des Produkt- und Serviceportfolios |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 3.9. *Landeskirchenübergreifende Transportverschlüsselung*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Es ist für bestimmte kirchliche Stellen im E-Mailverkehr eine landesübergreifende Transportverschlüsselung gemäß den Vorgaben der EKD umzusetzen. Diese Verschlüsselung garantiert eine vertrauliche Kommunikation zwischen den verschiedenen Landeskirchen. | | Bei der Versendung von vertraulichen E-Mails vom LKA der EKiR in Düsseldorf zur Kirchverwaltung der EKHN in Darmstadt wird eine einheitliche E-Mail-Transportverschlüsselung genutzt. Somit kann niemand auf dem Transportweg über das unsichere Internet den Inhalt dieser E-Mail lesen. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Eine vertrauliche Kommunikation per E-Mail über ein unsicheres Netz (Internet) ist nun möglich.<br><br>Die Transport-Verschlüsselung funktioniert unabhängig von Benutzereingriffen. Statt vielen Nutzenden müssen nur einzelne Administratoren geschult werden. | | Die eingesetzten E-Mail-Programme müssen so konfiguriert werden, dass diese einheitliche Transport-verschlüsselung automatisch aktiviert wird.<br><br>Es sind keine individuellen Einstellungen möglich, z. B. für digitale Signaturen. Diese Lösung kann nur für einzelne Gruppen von vorher festgelegten Kommunikationspartnern eingesetzt werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

# 4. *Non-Funktionale Anforderungen*

## 4.1. *Support*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Der Support ist der Service Desk. Es handelt sich um eine unterstützende Tätigkeit bei der Lösung von Problemen in der Nutzung von Programmanwendern. Der Support kann persönlich oder telefonisch erfolgen. Jeder Arbeitsbereich der EKIR kann seinen eigenen Service Desk haben oder es gibt einen zentralen Service Desk. I.d.R. gliedert sich der Service Desk in First, Second und Third Level Support.<br><br>First-Level Support: Die erste Ebene in einer Hierarchie von Support-Gruppen, die an der Lösung von Störungen (Incidents) beteiligt sind. Mit jeder Ebene sind mehr Know-how und Fertigkeiten von Experten vorhanden bzw. mehr Zeit oder andere Ressourcen verfügbar.<br><br>Second-Level Support, zweite Ebene in einer Hierarchie von Support-Gruppen, die mit der Lösung von Störungen (Incidents) und der Untersuchung von Problemen befasst sind.<br><br>Third-Level Support, dritte Ebene in einer Hierarchie von Support-Gruppen, die mit der Lösung von Störungen (Incidents) und der | • Pfarrer meldet den Ausfall seines PCs bei der Vor-Ort IT-Betreuung. (First Level Support). Die IT-Betreuung beauftragt den IT-Dienstleister, die Reparatur vor Ort durchzuführen (Second Level Support). |

| | | |
|---|---|---|
| Untersuchung von Problemen befasst sind. | | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Dienstleistungsorientierung der IT<br>• Sichtbarkeit und Wahrnehmung der IT innerhalb der EKIR<br>• Nutzerfreundlichkeit<br>• Anwenderbetreuung<br>• Sicherstellung des Incidentmanagements | • Höherer Administrationsaufwand<br>• Geregelte und vor allem bekannte Abläufe im Incident- und Problemmanagement<br>• Schulungsaufwand im Service Desk | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 4.2. *Ausfallhäufigkeit*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Die Ausfallhäufigkeit beschreibt die Anzahl von Fehlern bzw. Ausfällen in einem festgelegten Zeitraum. Sie dient als Maß für die Zuverlässigkeit der Groupwarelösung. Es ist eine objektiv messbare Größe. | • E-Mail Funktion steht innerhalb eines Monats | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Nutzerfreundlichkeit<br>• Nutzerakzeptanz<br>• Verfügbarkeit der Anwendung | • Bei hoher Ausfallhäufigkeit werden Nutzer die Anwendbarkeit bzw. den Sinn der Anwendung hinterfragen<br>• Marktreife der eingesetzten Lösung eruieren<br>• Ausreichendes Testing vor Inbetriebnahme | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 4.3. *Preis für Nutzung*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Der Preis für die Nutzung ist der Betrag, der für die Anwendung der Groupware an den Hersteller oder Lizenzgeber zu bezahlen ist. Es gibt verschiedene Lizenzmodelle als Berechnungsgrundlage. Alternativ kann die Anschaffung lizenzfreier Software sogenannter Open Source Lösungen in Erwägung gezogen werden. Wobei zu beachten ist, dass häufig eine Nutzung außerhalb des Privatgebrauchs nicht zulässig ist. | • Lizenz pro Arbeitsplatz<br>• Lizenz pro Nutzer/-in | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Wirtschaftlichkeit<br>• Rechtssicherheit | • Gefahr der Unter- oder Überlizenzierung durch Unkenntnis der Lizenzmodelle<br>• Kostenersparnis bei optimalen Einsatz<br>• Gefahr von Mehrkosten bei Überlizensierung | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 4.4. *Reaktionszeiten im Störfall*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Die Reaktionszeit beschreibt die Geschwindigkeit, mit der auf bestimmte Ereignisse reagiert wird. Dies könnte die Geschwindigkeit sein, mit der ein IT Service Provider auf eine Störung (Incident) oder Change Request usw. reagiert. Die Reaktionszeit beschreibt nicht den Zeitraum, der zur Lösung der Störung (Incident) oder zur Umsetzung des Change Requests benötigt wird, sondern z. B. den Zeitraum von der Störungsmeldung bis zum Beginn der ersten Reaktion. | • Pfarrerin meldet den Ausfall ihres PCs bei ihrem IT-Ansprechpartner / ihrer IT-Ansprechpartnerin. Diese/-r reagiert unmittelbar und bestätigt den Eingang der Fehlermeldung. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Kurzfristige Wiederherstellung der Funktion bzw. Inkrafttreten eines Workarounds<br>• Nutzerfreundlichkeit des Servicebereiches<br>• Nutzerakzeptanz | • Kurze Reaktionszeiten erfordern einen verfügbaren und geschulten Service und Support-Bereich<br>• Klarheit, wie und an wen die Störung gemeldet werden muss<br>• Standardisiertes Vorgehen im Störungsfall | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 4.5. *Support-Erreichbarkeit*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Support-Erreichbarkeit beschreibt den Kanal (E-Mail, Internetformular, Fax, Telefon etc.), wie ein/-e Betroffene/-r seine/ihre Stör- oder Fehlermeldung an eine/-n Servicemitarbeiter/-in weiterreicht bzw. zu welchen Zeiten der Support erreichbar ist.<br><br>Des Weiteren beschreibt es die Zeiten, zu denen der Support den Anwendern zur Verfügung steht. In der Regel bezieht sich dies auf die Zeiten, in denen der Service Desk erreichbar ist. Support-Stunden sollten in einem Service Level Agreement definiert werden. Sie können von den Servicestunden abweichen. Beispielsweise könnten sich die Servicestunden über 24 Stunden pro Tag, Support-Stunden hingegen auf die Zeit zwischen 07:00 und 19:00 Uhr erstrecken. | | • Fehlermeldung via Telefon, Fax |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Dienstleistungsorientierung der IT<br>• Nutzerfreundlichkeit<br>• Bedarfsgerechter und definierter IT-Support zur Ermittlung der benötigten Ressourcen | | • Kenntnis über die Spitzenzeiten für Anfragen an den Support<br>• Ausreichende Mitarbeiterbereitstellung im Support<br>• Klarheit über Eingangskanäle zum Support<br>• Geregelte und vor allem bekannte Abläufe im Incident- und Problemmanagement |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 4.6. *Wiederherstellungszeiten*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Zeit, welche für die Wiederherstellung nach einem Ausfall benötigt wird, wird ab dem Zeitpunkt des Ausfalls bis zur vollständigen Wiederherstellung der normalen Funktionalität gemessen. | | • E-Mail Funktion ist eine halbe Stunde nach Meldung der Störung durch einen EKIR Mitarbeiter wieder verfügbar. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Nutzerfreundlichkeit<br>• Nutzerakzeptanz<br>• Schnellstmögliche Wiederverfügbarkeit der Anwendung | | • Kurze Wiederherstellungszeiten erfordern einen verfügbaren und geschulten Service und Support Bereich<br>• Ggf. erhöhter Personal- und Kostenaufwand |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 5. *Sicherheitsanforderungen*

### 5.1. *Softwareaktualisierung*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Regelmäßiges und zeitnahes Einspielen aktueller Sicherheits-Patches, die entsprechende Sicherheitslücken beheben, sollte gewährleistet sein. Dies gilt zum einen für das jeweilige Betriebssystem (z.B. Windows XP, Windows Vista, Windows Server 2008 oder Linux). Ein regelmäßiges und zeitnahes Patchen der E-Mail-Software (z.B. Outlook, Mozilla Firefox, etc.) ist ebenso vorzunehmen.<br><br>Auf den PCs und Notebooks ist die Updatefunktion auf automatisch einzustellen oder die Aktualisierung regelmäßig (mindestens alle zwei Wochen) durchzuführen. | | Die Mitarbeitenden haben die automatische Updateversion ihres Betriebssystems aktiviert. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Das Kompromittieren der E-Mail-Systeme kann durch die Aktualisierung sehr minimiert werden. | | Eine Mitarbeitendeninformation muss kirchenweit durchgeführt werden.<br><br>Vorgaben zum Update- und Änderungsmanagement (engl. change management) müssen in der Sicherheitskonzeption aufgenommen werden.<br><br>Das regelmäßige Ausführen von Update oder Patch auf zentralen Komponenten darf nicht zu einem Betriebsausfall führen. (Cluster) |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.2. *Zugangsreglung Betriebsräume*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Kirchliche Rechenzentren bzw. Serverräume, in denen wichtige IT-Systeme situiert sind, müssen gemäß BSI-Grundschutz gesichert werden. Dazu zählen Aspekte wie z.B.:<br><br>• Vorhandensein von Brandschutzanlagen/Handfeuerlöscher,<br>• Sichere Aufteilung der Stromkreise<br>• Ausreichende Klimatisierung<br>• Lokale Unterbrechungsfreie Stromversorgung (USV)<br>• Technische und organisatorische Vorgaben für Serverräume<br>• Zutrittsregelungen und -kontrolle<br>• Geschlossene Fenster und Türen<br>• Vermeiden von wasserführenden Leitungen | | Die Serverräume des LKA in Düsseldorf benötigen einen hohen Sicherheitsstandard, da dort viele Systeme mit hohem Schutzbedarf situiert sind.<br><br>Im Sekretariat der Kirchengemeinde sollte beim Verlassen immer abgeschlossen und eventuelle offene Fenster geschlossen werden. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Wichtige Dokumente und IT-Systeme werden damit effektiv vor Diebstahl geschützt. | | Es muss eine Mitarbeitendeninformation erstellt und bekannt gemacht werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.3. *Sichere Passwörter*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Für die Passwortgestaltung gelten die folgenden Vorgaben:<br><br>• Voreingestellte Passwörter müssen durch individuelle Passwörter ersetzt werden.<br>• Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.<br>• Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben und Zahlen bestehen.<br>• Es sollte mindestens 8 Zeichen lang sein.<br>• Passwörter müssen geheim gehalten werden und sollten nur dem Benutzer persönlich bekannt sein.<br>• Das Passwort muss regelmäßig gewechselt werden.<br>• Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.<br>• Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden.<br>• Die Eingabe des Passwortes sollte unbeobachtet stattfinden. | Ein Passwort der Form „abc123“ entspricht nicht den zuvor beschriebenen Anforderungen.<br><br>Ein gültiges Passwort wäre zum Beispiel das folgende aus dem Satz „Kollegin Gabi kommt morgens immer 7 Uhr.“ „KGkim7Ud“ abgeleitete Passwort.<br><br>Dieser Satz kann durchaus im Gegensatz zum blanken Passwort auf einem Zettel notiert sein, ohne dass Dritte Kenntnis davon bekommen. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Die Sicherheit der Authentisierung ist entscheidend davon abhängig, dass die Passwörter korrekt gebraucht werden. | Es ist unbedingt notwendig bei der Einführung der Anforderungen des Passwortgebrauchs die IT-Nutzenden diesbezüglich zu unterweisen.<br><br>So weit wie möglich sollte die Einhaltung der Regelungen auch durch technische Prüfungen (Passwortlänge, Ablauf eines Passwortes, |

| | | |
|---|---|---|
| | Passworthistorie) werden. | vorgenommen |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.4. *Schulung zu Sicherheitsmechanismen für Benutzer*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Benutzer müssen vor dem Einsatz von Kommunikationsdiensten und Groupware-Applikationen wie E-Mail geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der kirchlichen Sicherheitsanforderungen zu gewährleisten. | | Dies könnte z. B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein ungewöhnliches Verhalten der Kommunikationssoftware gemeldet werden soll. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Bei der Sicherheit kommt es oft auf jedes Glied in der Kette an, damit Sicherheit auch umgesetzt ist. Die beste technische Sicherheitsmaßnahme nützt nichts, wenn der bedienende Mensch sie mit oder ohne Absicht umgeht. | | Die Mitarbeitenden müssen für die sichere Anwendung von E-Mail und Groupware informiert und sensibilisiert werden |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.5. *Rollen- und Berechtigungskonzept (Zugang, Vertretungsregelungen auf Postfächer, Funktionspostfächer)*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Ein Berechtigungs- und Rollenkonzept muss folgende Aspekte der E-Mail-Nutzung beinhalten:<br><br>• Es muss einen dokumentierten Prozess geben, wie und unter welchen Voraussetzungen ein Mitarbeitender eine kirchliche E-Mail-Adresse und ein Postfach bekommt. Dabei muss es auch eine Regelung für den Entzug/das Deaktivieren eines Postfaches geben.<br>• Jedes persönliche Postfach/ jedeE-Mail-Adresse darf nur einem Mitarbeitenden zugordnet werden, auf welches nur er Zugriff haben darf. Passwörter dürfen nicht weitergegeben werden.<br>• Es müssen Vertreter für alle längeren Abwesenheitsphasen benannt werden. Dies kann auch Externen über solche Mechanismen wie den Abwesenheitsassistent mitgeteilt werden, so dass sie wissen, dass die E-Mail angekommen ist und bearbeitet wird.<br><br>Um unberechtigte Zugriffe zu vermeiden, ist das | Ein Mitarbeitender stellt einen Antrag auf Erteilung eines persönlichen E-Mail-Kontos und einer E-Mail Adresse.<br><br>Ein Mitarbeiter schaltet vor seinem Jahresurlaub eine Abwesenheitsschaltung, in der seine Vertretung mit E-Mail-Adresse genannt wird.<br><br>Die Administratoren überprüfen das Berechtigungskonzept mindestens einmal im Jahr. |

| | | |
|---|---|---|
| Berechtigungskonzept regelmäßig zu prüfen. | | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| Eine klare Konzeption für Rechte und Rollen hilft dabei, Missverständnisse und Fehlnutzung durch eine strukturierte Regelung zu vermeiden. | Das Rollen- und Berechtigungskonzept muss erstellt und regelmäßig überprüft werden. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 5.6. *Vertraulichkeit*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Bei der Übermittlung von sensiblen Daten mittels E-Mail, insbesondere über kirchliche Grenzen hinweg, sollten diese Daten entsprechend ihrer Sicherheitseinstufung (auch Informationsklassifizierung) vertraulich kommuniziert werden, d.h. verschlüsselt und elektronisch signiert werden.<br><br>Vertraulich heißt in diesem Sinne, dass nur autorisierte Personen Zugriff auf diese klassifizierten Daten haben sollen. | | Das als „vertraulich“ eingestufte Protokoll der letzten Presbyter-Sitzung wird den Teilnehmern verschlüsselt übersendet, da sensible Daten enthalten sind. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Vertraulichkeit muss genauso wie im persönlichen Gespräch oder traditionellen Briefpostverkehr auch per E-Mail gewährleistet werden. | | Die organisatorischen und technischen Voraussetzungen müssen geschaffen werden, um eine Sicherheitseinstufung durchzuführen.<br><br>Ein Vorgehen zur Sicherheitseinstufung muss entwickelt werden.<br><br>Die Sicherheitseinstufung von Dokumenten muss von den relevanten Mitarbeitenden vorgenommen werden.<br><br>Anforderungen an zentrale PKI beachten |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Muss |

## 5.7. *Integrität (Schutz vor Manipulation, Formatänderung)*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Bei der Übermittlung von sensitiven Daten mittels E-Mail, insbesondere über kirchliche Grenzen hinweg, sollten diese Daten entsprechend ihrer Sicherheits-Einstufung (auch Informationsklassifizierung) integer übermittelt werden, d.h. elektronisch signiert werden.<br><br>Integrität heißt in diesem Sinne, dass die Daten korrekt (unversehrt, nicht manipuliert) durch korrekt funktionierende Systeme übertragen werden. | | Die wöchentliche Liste der eingesammelten Kollekte wird per E-Mail unter Wahrung der Integrität an das Verwaltungsamt übermittelt. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Die Wahrung der Integrität von Daten ist eine rechtliche Anforderung an die E-Mail-Systeme, die für verlässliche Daten unerlässlich ist. | | Technische Voraussetzungen für die Signierung von E-Mails müssen gegeben sein. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Muss |

## 5.8. *Verfügbarkeit*

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Die Anforderungen an die E-Mail-Verfügbarkeit muss anhand der entsprechenden Arbeitsaufgaben abgeleitet werden. Um diese Anforderung sinnvoll abzuleiten, ist zu klären, welche Arten von Informationen über welche Wege über das E-Mail- bzw. Goupware-System kommuniziert werden sollen und welchen Schutzbedarf diese Informationen und die damit zusammenhängenden Arbeitsaufgaben haben. | Die Seelsorge per E-Mail bezüglich Lebenskrisen sollte aufgrund der Dringlichkeit eine hohe Anforderung an die Verfügbarkeit (z.B. kleiner als 1 Stunde) haben. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| Die Verfügbarkeit ist in einigen kirchlichen Bereichen wichtiges Sicherheitsziel, das umgesetzt werden muss. | Eine genaue Aufnahme zeitkritischer E-Mail-Kommunikation muss erstellt werden. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 5.9. *Festplattenverschlüsselung bei dienstlichen Geräten*

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Eine Festplattenverschlüsslung von dienstlichen Geräten ist dann gefordert, wenn diese Geräte sensible Daten gespeichert haben und diese Geräte in der Öffentlichkeit aufgestellt bzw. unbemerkt von Fremden entwendet werden könnten. Eine Festplattenverschlüsselung sorgt dafür, dass Inhalte, die auf mobilen Festplatten oder Speichern lagern, nur von autorisierten Personen gelesen und verarbeitet werden können. Zudem ist auf solchen Geräten ein ausreichender Zugriffsschutz zu gewährleisten. Eine automatische Sperrung des Zugriffs und eine anschließende Entsperrung mit Passwort oder PIN wird gefordert.<br><br>[OPTIONAL: Neu anzuschaffende mobile Rechner ,die viel außerhalb der kirchlichen Gebäude im Einsatz sind und auf denen personenbezogene Daten gespeichert werden, müssen mit einer Festplattenverschlüsselung ausgestattet werden.] | Der Gemeinderechner, auf dem die Liste aller Gemeindemitglieder und Adressen gespeichert sind, steht in einem nicht abgeschlossenen Arbeitsraum direkt neben der Ausstellung, die von vielen Personen auch außerhalb der Gemeinde besucht wird. Jede Person könnte unbemerkt an den Rechner und sich diese personenbezogene Datei kopieren. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Datenschutzgesetze und IT-Sicherheit würden mit der Umsetzung beachtet und das Risiko einer Schadensersatzklage oder eines Imageverlustes wird minimiert. | Eine Festplattenverschlüsselung ist nicht immer möglich bzw. erfordert Know-How von IT-Experten. Zudem müssen wiederum Sicherheits-anforderungen beim Einsatz von Festplattenverschlüsselung beachtet werden. |
| | **offene Inhalte** / **vertrauliche/schützenswerte Inhalte** |

| Verbindlichkeitsgrad | Soll | Muss |
|---|---|---|

## 5.10. *Schulung zur Systemarchitektur und Sicherheit für Administratoren*

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Administratoren, die für die Verwaltung von Benutzerkennungen, Rollen, Profilen oder Berechtigungen verantwortlich sind, müssen zwingend Schulungen zum Berechtigungskonzept und zur Berechtigungsverwaltung (Vorgehen, Werkzeuge, richtige Verwendung) erhalten oder die entsprechenden Kenntnisse nachweisen. Nur so wird erreicht, dass die Berechtigungsverwaltung versiert durchgeführt werden kann.<br><br>Außerdem sollten die Administratoren durch Teilnahme an Schulungsmaßnahmen wie Seminare oder Anwendertagungen entsprechend ihren Aufgaben ausgebildet werden. Es sollte überlegt werden, die Ausbildung anhand eines Schulungsplanes festzulegen. | | Folgende Themen sollten z.B. in Schulungen behandelt werden:<br><br>• Aktuelle Gefährdungen von Groupware-Systemen<br>• Überblick über SMTP-Sicherheit<br>• Abwehr von Schadsoftware und Spam<br>• Überblick über rechtliche Aspekte bei der Administration, wie z. B. Datenschutz<br>• Einrichten von Berechtigungen<br>• Überblick über die Lösungen für die Nachrichtensicherheit, z. B. Verschlüsselung, Digitale Signatur, VPNs, Protokollierung<br>• Sicherung und Verwaltung von Konfigurationsdaten<br>• Datensicherung<br>• Incident Handling und Disaster Recovery Maßnahmen |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| In diesen Themen geschulte Administratoren sind unverzichtbar für einen sicheren IT-Betrieb. | | Ein Schulungsplan bzw. ein Schulungsbudget muss zur Verfügung stehen.<br><br>Bei der Einstellung von Administratoren sind die Fähigkeiten zu prüfen. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## *Anhang – Überblick Verbindlichkeit*

| Anforderungsbereich | Anforderung | offene Informationen | vertraulich/schüt Informatio |
|---|---|---|---|
| **Betrieblich** | Nutzung von Standardprotokollen | Muss | Muss |
| | Skills/Wissen IT Personal | Muss | Muss |
| | On-/Offboarding | Muss | Muss |
| | Wirtschaftlichkeit im Betrieb | Soll | Soll |
| | Schnittstellen/ Datenaustausch bei verteilten Betriebsstandorten | Soll | Muss |
| | API-Schnittstellen | Kann | Kann |
| | Datenübernahme von anderen Systemen | Kann | Kann |
| **Gesetzlich** | Anforderungsprofil und Programmdokumentation | Muss | Muss |
| | Gewährleistung der IT-Sicherheit | Muss | Muss |
| | Gewährleistung des Datenschutzes | Muss | Muss |
| | Gewährleistung Lizenzsicherheit | Muss | Muss |
| | Test der Anwendung | Muss | Muss |
| | Wirtschaftlichkeit | Muss | Muss |
| | Berücksichtigung der BSI Anforderungen | Soll | Soll |
| | Erstellung Sicherheitskonzept | Muss | Muss |
| | Gewährleistung rechtssichere Archivierung | Soll | Soll |
| | Verhaltensregeln bei Verdacht auf Sicherheitsvorfall | Soll | Soll |
| | Verschlüsselung schützenswerter Daten | Kann | Muss |
| **Kirchenspezifika** | Anerkennung des EKD-DSG | Muss | Muss |
| | Ausschuss für öffentliche Verantwortung | Soll | Soll |
| | Eigenerklärung | Soll | Soll |
| | Verpflichtung Scientology | Soll | Soll |
| | Frieden und Gerechtigkeit | Soll | Soll |

| Anforderungsbereich | Anforderung | offene Informationen | vertraulich/schüt Informatio |
|---|---|---|---|
| | Wahrung der Schöpfung | Soll | Soll |
| | Wiederverwendbarkeit landeskirchlicher-übergreifender Lösungen | Soll | Soll |
| | Nachhaltigkeitsnachweis | Soll | Soll |
| | Landeskirchenübergreifende Transportverschlüsselung | Soll | Soll |
| | Betriebsstandorte | Kann | Kann |
| **Non-funktional** | Support | Muss | Muss |
| | Ausfallhäufigkeit | Soll | Soll |
| | Preis pro Nutzung | Soll | Soll |
| | Reaktionszeiten im Störfall | Soll | Soll |
| | Support-Erreichbarkeit | Soll | Soll |
| | Wiederherstellungszeiten | Soll | Soll |
| **Sicherheit** | Softwareaktualisierung | Muss | Muss |
| | Zugangsregelung für Betriebsräume | Muss | Muss |
| | Sichere Passwörter | Muss | Muss |
| | Schulung zu Sicherheitsmechanismen für Benutzer | Muss | Muss |
| | Rollen- und Berechtigungskonzept | Soll | Soll |
| | Vertraulichkeit | Soll | Muss |
| | Integrität | Soll | Muss |
| | Verfügbarkeit | Soll | Soll |
| | Festplattenverschlüsselung bei dienstlichen Geräten | Soll | Muss |
| | Schulung zur Systemarchitektur und Sicherheit für Administratoren | Soll | Soll |

# Ergänzende Anforderungsbeschreibung Groupware

*Hinweis:*

*Dieses Dokument befindet sich im Entwurfsstadium.*

# *Inhalt*

## *Einführung*

Das folgende Dokument bietet ihnen eine Übersicht der ergänzenden Anforderungen einer in der Evangelischen Kirche im Rheinland (EKiR) eingesetzten Groupwarelösung. Eine Groupwarelösung bezeichnet eine Software, die die Zusammenarbeit in einer Gruppe über eine zeitliche oder räumliche Distanz gewährleistet. Die bekanntesten Groupwarefunktionen sind E-Mail, Kalender und Adressverzeichnisse.

Die ergänzenden Anforderungen für eine Groupwarelösung bauen direkt auf den Basisanforderungen für IT-Systeme in der EKiR auf (*Dokument: Beschreibung der Basisanforderungen für IT Systeme in der Evangelischen Kirche im Rheinland*). Sie gelten für alle Nutzenden der eingesetzten Groupwarelösung.

Hinsichtlich des Aufbaus des Baukastensystems der IT-Standards und des Aufbaus dieser Dokumentation sei auf das oben genannte Dokument „Basisanforderungen“ verwiesen.

## 1. Betriebliche Anforderungen

### 1.1. Erreichbarkeit von Mail-Verteiler-Listen (intern/extern)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Erreichbarkeit von Mail-Verteiler-Listen beschreibt die Sichtbarkeit bzw. Verfügbarkeit von intern eingesetzten E-Mailverteilern durch Außenstehende. Mailverteiler bieten die Möglichkeit einer zweckmäßigen Zusammenfassung von verschiedenen Empfängerkreisen mit gleichem Informationsbedarf. Die Mail-Verteiler-Listen können dabei alle Mitglieder der EKiR beinhalten oder Teilbereiche. Durch den Einsatz von Smartphones kommt es bei einigen Apps zu Abfragen des Adressbuches. Dabei werden die Kontaktlisten bspw. mit den Kontakten in Sozialen Netzwerken abgeglichen. | | • Der E-Mail-Verteiler „alle@ekir.de“ sollte außerhalb der Organisation nicht verwendbar sein |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Verhinderung von ungewollten Massenmailings<br>• Datenschutz<br>• SPAM Schutz<br>• Vermeidung von Schaden an der IT Infrastruktur durch eingegangene Schadprogramme<br>• Vermeidung des Blacklistings durch unsachgemäße Benutzung | | • Sicherstellung der Nichtveröffentlichung von internen E-Mail-Verteilern auf öffentlichen Plattformen der EKiR<br>• Standardisierte Vorgehensweisen im Umgang mit E-Mail-Verteilerlisten |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2. *Funktionale Anforderungen*

### 2.1. E-Mail

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Durch die Funktion „E-Mail“ können Informationen und Nachrichten über das Internet versendet und empfangen werden. In den Einrichtungen innerhalb der EKIR werden E-Mail-Funktionalitäten genutzt, um sowohl offene Inhalte als auch vertrauliche und schützenswerte Informationen auszutauschen. | | • Presbyter für Öffentlichkeitsarbeit informiert Gemeindemitglieder über kommende Veranstaltungen.<br>• Presbyter tauschen sich über Diskussionspunkte der letzen Presbyteriumssitzung aus. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Schneller und ortsunabhängiger Austausch von Informationen<br>• Informationsverteilung an eine Vielzahl von Empfängern möglich<br>• Kostengünstige Form des Informationsaustauschs<br>• Geringerer Aufwand sowohl bei Erstellung, Versendung als auch Empfang<br>• Direkte Reaktion möglich<br>• Bei Verwendung von Pseudonymen höhere Anonymität möglich | | • Beachten von Sicherheitsstandards<br>• Gefahr des sorglosen Umgangs (E-Mail wird häufig analog der Vertraulichkeit eines Briefes eingesetzt, obwohl in der Regel eine offene Postkarte die treffendere Analogie wäre)<br>• Einfache Weitergabe von vertraulichen Inhalten an Unbeteiligte und/oder Unbefugte<br>• Ungewollte Weitergabe von Schad-programmen bspw. Viren oder Trojaner<br>• Ungewollte Weitergabe von Adressdaten an Unbeteiligte und/oder Unbefugte |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.2. Kalender

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Der Kalender ist die zentrale Terminsteuerungs- und -planungsfunktion der Groupwarelösung. Die Kalenderfunktion gibt den Mitarbeitern und Mitarbeiterinnen der EKiR die Möglichkeit der Vereinbarung von Terminen bzw. der Terminanfragen an Kollegen oder externe Dienstleister. Empfangene Termine können abgelehnt und bestätigt werden. Darüber hinaus kann man die Zu- oder Absage eines Termins kommentieren. Termine lassen sich über die Vorschauansicht im Kalender anzeigen. Es besteht die Möglichkeit der Antwort mit Alternativvorschlag. Zudem stehen verschiedene Ansichten des Kalenders zur Verfügung. | • Pfarrerin lädt Gemeindeglieder zum Gedankenaustausch ein<br>• Vereinbarung einer Kirchenkreissitzung<br>• Terminierung der Kreis- oder Landessynoden | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • jederzeit Zugriff auf den gesamten Kalender auch vergangener Jahre<br>• Schnelle und ortsunabhängige Terminierung<br>• gleichzeitiges Versenden einer Terminanfrage an mehrere Adressaten<br>• Prüfungen von freien Terminen<br>• Geringerer Aufwand sowohl bei Erstellung, Versendung als auch Empfang<br>• Direkte Reaktion möglich | • Standardisierte Verhaltensregeln für das Einladen und Versenden von Terminen<br>• Prüfung der Relevanz für die Empfänger<br>• Ungewollte Weitergabe von vertraulichen Inhalten an Unbeteiligte oder Unbefugte<br>• Jeweils Festlegung wie An- und Abreisezeiten zu erfassen sind<br>• Die Möglichkeit, Zeiten der Abwesenheit ohne Grund (private Termine) einzugeben, muss gewährleistet sein.<br>• Standardisiertes Format für den Datenaustausch notwendig (z.B. ics)<br>• Plattformunabhängigkeit notwendig | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.3. Kontakte

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Kontakte innerhalb einer Groupware sind das elektronische Adressbuch des Nutzenden. Die Vielzahl an Kontaktinformationen wird durch die Nutzung der Kontaktverwaltung in Groupwarelösungen vereinfacht. Egal, ob es sich um einen neuen, einen veränderten oder einen nicht mehr benötigten Kontakt handelt, der/die Nutzer/in hat die Möglichkeit, diese Veränderung ohne großen Aufwand durchzuführen. | | • Neuanlegen eines Pfarrers<br>• Gruppierung aller Mitglieder der Landesynode<br>• Löschung der Daten eines verstorbenen Gemeindeglieds<br>• Möglichkeit, mehrere Adressbücher zu führen (private /geschäftliche Kontakte) muss gegeben sein |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Zugriff auf die Daten von internen und externen Kirchenkontakten<br>• Unkompliziertes Anlegen, Ändern und Löschen von Kontaktdaten<br>• Bequemes Handling von großen Datenmengen<br>• Vielzahl von Kontaktmöglichkeiten auf einen Blick (Adresse, E-Mail, Telefon, Handy (dienstlich und privat?) etc.)<br>• Kontaktinformationen gemeinsam nutzen<br>• Zusammenfassen von Kontakten zu Gruppen | | • Standardisierte Verhaltensregeln für die Nutzung und Freigabe von Kontakten<br>• Einhaltung der gesetzlichen und kircheninternen Datenschutzrichtlinien<br>• Prüfung der Relevanz für die Empfänger<br>• Ungewollte Weitergabe von vertraulichen Daten an Unbeteiligte oder Unbefugte<br>• Berechtigungskonzept für Zugriffe auf Daten oder Bestandteile notwendig (z.B. VIP-Personen)<br>• Definition von Pflichtfeldern bei Anlage von Kontaktdaten<br>• Revision von Kontaktdaten / Ablauf (Löschung) muss hinterlegbar sein |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.4. Funktionale Postfächer

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Ein Funktionspostfach ist ein nicht personengebundenes E-Mail Postfach, das an eine kirchliche Funktion und/oder Einrichtung gebunden ist. Dabei können eine oder mehrere Personen Zugriff auf den Inhalt haben. Das Funktionspostfach kann im E-Mail-Client der Mitarbeitenden eingebunden oder auf einem separaten Rechner eingerichtet werden. | | • Erreichbarkeit bei wechselndem Personal<br>• nicht personengebundene Kontaktdaten auf öffentlichen Webseiten der E-KiR (info@..., chatseelsorge@ekir... oder kirchenkreis@...) |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • bei Unkenntnis des Nutzenden hinsichtlich der Ansprechpartner<br>• Aufrechterhaltung des Informations-austauschs auch bei wechselnden Ansprechpartnern<br>• unkompliziertes Sammeln von Informationen ohne personellen Bezug<br>• Vermeidung von unnötigen Informationen im persönlichen Postfach durch die Angabe von funktionalen E-Mailadressen | | • Gewährleistung des Datenschutzes hinsichtlich Vertraulichkeit des Inhalts und Kontaktdaten des Versenders<br>• Sicherstellung der Reaktion auf das Anliegen des Versenders, ggf. Weiterleitung an zuständige Person<br>• Absender/-in ist nicht bewusst, an wen sie/er adressiert<br>• Verantwortung für den Empfang ist organisiert und geregelt<br>• Verantwortung, wer ein funktionales Postfach anlegt<br>• Wer trägt die Hauptverantwortung hinsichtlich Bearbeitung?<br>• Der Personenkreis hinter einer Funktions-adresse muss jederzeit qualifizierbar und dokumentiert sein. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.5. Assistenzfunktion

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Assistenzfunktion unterstützt die Kommunikation bei Abwesenheit der/des E-Mail-Empfängers/Empfängerin. So kann z. B. eine Meldung mit Grund und Dauer der Abwesenheit an die absendende Stelle erzeugt werden, Verfügbarkeiten können im Kalender angezeigt werden. Bei modernen Groupwarelösungen kann man gesondert Abwesenheitsnotizen an firmeninterne und externe Mailversender verschicken. Weitere typische Funktionen sind die Ordnerfreigabe und Assistenzfunktionen wie das "Senden im Auftrag". | | • Pfarrer ist im Urlaub und erhält via Email eine Terminanfrage für ein Taufgespräch<br>• Verwaltungsleiterin ist erkrankt und kann E-Mails in dieser Zeit nicht persönlich bearbeiten |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Sicherstellung einer verlustfreien Übernahme von Kommunikation, Terminen und Aufgaben bei Abwesenheit eines Mitarbeiters/einer Mitarbeiterin durch eine/n festgelegte/n Kollegen/in. | | • Standardisierte Verhaltensregeln hinsichtlich der Stellvertreterrolle in der Nutzung des Groupwarezugangs.<br>• Datenschutzrechtliche Prüfung notwendig<br>• Organisatorische Anforderungen beachten (Zustimmung der Mitarbeitenden, ungeplante Abwesenheiten, Dokumentation) |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.6. Webmail Zugriff

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | **Beispiele** | |
| Der Webmail Zugriff beschreibt die Möglichkeit auf die E-Mail mittels eines Webbrowsers zuzugreifen. Dabei ist es nicht notwendig vor dem eigenen Computer zu sitzen, sondern von jedem Rechner können über ein Browserprogramm, wie dem Internetexplorer oder Firefox, E-Mails, Kalenderinformationen oder Kontakte aufgerufen werden. | • Abruf der E-Mails über den HeimPC des Mitarbeitenden | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Orts- und systemunabhängige Benutzung der Groupwarelösung<br>• Kosteneinsparung bei der Infrastruktur | • Standardisierte Verhaltensregel im Umgang mit und bei Benutzung von Webmail<br>• Ungewolltes Hinterlassen von Zugangsinformationen auf Fremdrechnern<br>• Höhere Sicherheitsstandards für die IT Infrastruktur<br>• Prüfung Verfahren Browser-VPN not-wendig. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.7. Multiple Domainen

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Multiple Domainen beschreiben die Möglichkeit ,mehrere Webseiten auf dem gleichen Hostingpaket zu betreiben. Es besteht so die Möglichkeit, dass ein/e Mitarbeiterin der EKiR verschiedene E-Mail Adressen hat, diese aber alle in einem Postfach zusammenlaufen. | | • Direktes Zustellen dienstlicher E-Mails, währenddessen Newsletter oder Werbung nur einmal am Tag abgerufen werden |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Globaler Speicherplatz<br>• Einsparung von Verwaltung mehrerer Hostings mit unterschiedlichen Zugängen und Laufzeiten<br>• Erreichbarkeit eines Postfaches über verschiedene E-Mail Adressen<br>• Auswertbarkeit von E-Mail-Adressen von Mitarbeitenden<br>• Trennung zwischen interner und externer Kommunikation | | • Erhöhter Pflege- und Administrations-aufwand |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 2.8. Räume und Ausstattungsgegenstände

| Version 0.9 vom 04.06.2013 | |
|---|---|
| **Beschreibung** | **Beispiele** |
| Für die Organisation und Durchführung von Besprechungen steht in den Dienstgebäuden der kirchlichen Einrichtungen nur eine begrenzte Anzahl an Besprechungsräumen zur Verfügung.<br>Eine Funktion „Raumsuche“ mit Einbindung in die Kalenderfunktionalität und Besprechungsplanung kann dazu genutzt werden, freie Räumlichkeiten zu erkennen und diese für die Durchführung einer Besprechung zu reservieren. Bei Bedarf kann diese Funktionalität auch um die Reservierung von Ausstattungsgegenständen genutzt werden. | • Raumsuche im Rahmen der Organisation einer Besprechung in einem Gebäude der Kirchenverwaltung<br>• Reservierung von Beamer, Flipchart und Moderationsausstattung im Rahmen der Organisation einer Besprechung in einem Gebäude eines Kirchenkreises |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Direkte Suchmöglichkeit nach freien Räumen und Ausstattungsgegenständen durch die Besprechungsorganisation<br>• Direkte Übersicht aller verfügbaren Räume und freien Ausstattungsgegenstände<br>• Buchen und Reservieren von Räumen und Ausstattungsgegenständen<br>• Sichtbarmachen von freiwerdenden Räumen und Ausstattungsgegenständen aufgrund von Absage und Stornierung<br>• Effiziente Raumauslastung, Reduzierung von Leerständen und Vermeidung von überlappenden Mehrfachbuchungen<br>• Über Auswertungen Sichtbarmachung von Ausstattungsbedarfen (z. B. Anzahl Beamer, Austausch Material Moderationskoffer) | • Standardisierte Nutzungsregeln für das Buchen und Reservieren von Räumen und Ausstattungsgegenständen<br>• Rechtevergabe für das Buchen und Reservieren<br>• Stammdatenpflege von Räumen und Ausstattungsgegenständen inkl. laufender Aktualisierung<br>• Priorisierung der Dringlichkeiten (Verfahren bei Anfragenkollisionen)<br><br>Hinweis: In der Regel nur bei größeren Nutzerzahlen und entsprechendem Raumangebot sinnvoll. |

| | offene Inhalte | vertrauliche/schützenswerte Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Muss |

## 2.9. Zugriff auf E-Mail-Archiv

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die meisten E-Mail und Groupware-Lösungen unterscheiden den Posteingang und das E-Mail-Archiv. Während neu eingehende E-Mails im Posteingang abgelegt und von dort bearbeitet werden können, sollten bearbeitete E-Mails aus diesem entfernt und in das Mail-Archiv überführt werden. Vergleichbar ist dies mit der Briefpost: Der private Hausbriefkasten (Posteingang) wird in der Regel täglich geleert. Die neue Post wird gesichtet, einiges direkt entsorgt und einiges nach dem Bearbeiten in Ordner abgeheftet (Archiv).<br><br>In den Groupware-Lösungen werden aus dem Posteingang in regelmäßigen Abständen (z. B. im Zeitablauf oder bei Erreichen einer def. Postfachgröße) E-Mails gefiltert und möglichst automatisiert in eine Ablage ausgelagert und somit aus dem Postfach entfernt.<br><br>Anforderung an den Funktionsumfang der E-Mail-Lösung ist es, dass aus dem E-Mail-Programm auch nach dem Verschieben der E-Mail aus dem Postfach in das Archiv auf diese archivierten E-Mails zuggegriffen werden kann. | • Mailverkehr des vergangenen Jahres und/oder noch älter im Ordner „Archiv“ unter Outlook<br>• Funktion „Archivieren“ bei GoogleMail / Gmail |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Rückverfolgung von E-Mails aus älteren Bearbeitungs- und Kommunikationsvorgängen | • Standardisierte Verhaltensregeln hinsichtlich Speichern und Archivierung von Alt-E-Mails.<br>• Turnusfestsetzung hinsichtlich Alter und |

| | |
|---|---|
| • Kleinhalten des Postfachs (Briefkastenleerung vs. Ablage)<br>• Verbesserung der Wirtschaftlichkeit(Kosten des Postfachs in der Regel höher als Kosten des Archivs)<br>• Archive einfacher in Sicherungsverfahren übernehmen<br>• Ladezeiten / Netzressourcen schonen<br>• Vermeidung von unübersichtlichen Ablageordnern | Verschieben von E-Mails in das Archiv.<br>• Umdenken in der Arbeitsweise<br>• Limitierung von Postfachgrößen<br>• Verfahren von Archivierungssystem<br>• Höherer Supportbedarf (Wo ist meine E-Mail?)<br>• Gesetzliche Anforderung an eine E-Mail-Archivierung prüfen und klassifizieren.<br>• Konkurrierende DMS-Systeme / Rang klären.<br>• Zugriff via Webbrowser (Portallösung) prüfen |

| | offene Inhalte | vertrauliche/schützenswerte Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.10. Einbinden mehrerer Adressverzeichnisse

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Groupwarelösungen bieten die Möglichkeit diese Daten aus verschiedenen Quellen in ein gemeinsam genutztes System zu überführen und somit zentral bereitzustellen. Adress- und Kontaktdaten werden in den Einrichtungen der EKIR heute in unterschiedlichen Verzeichnissen gespeichert und gepflegt. | Aufbau eines gemeinsames Adressverzeichnisses aller hauptamtlich tätigen Personen innerhalb der EKIR in einem kircheneinrichtungsübergreifenden Adressverzeichnis |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Automatisierte Übernahme von Kontaktdaten aus bestehenden Lösungen ohne Doppelerfassung<br>• Einlesen loser Sammlungen bspw. aus Excel Tabellen<br>• Auslesen der Daten und damit Synchronisation mit mobilen Endgeräten<br>• Zentrale und Kircheneinrichtungs-übergreifende Nutzung der Adressinformationen<br>• Vermehrte Nutzung zentraler Adress-verzeichnisse | • Datenschutzrechtliche Prüfung notwendig<br>• Definition von „führenden Systemen“ – Verfahren bei Änderungen |

| | offene Inhalte | vertrauliche/schützenswerte |
|---|---|---|

| | | Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.11. Anbindung an / von Fachanwendungen

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | **Beispiele** | |
| Die Funktion Anbindung an/von Fachanwendungen beschreibt die Nutzung der Groupware-Funktionen (z. B. E-Mail) durch andere Fachanwendungen (z. B. Finanzwesen, Meldewesen). Es besteht die Möglichkeit, Daten und Informationen direkt aus der Fachanwendung per E-Mail zu versenden. Die E-Mail Funktion ist bspw. mit dem Meldewesen verknüpft und ermöglicht eine direkte Verschickung der Informationen aus der Meldewesensoftware. | • Erstellung eines Kontaktes aus dem Meldewesen (Datenübergabe)<br>• E-Mail-Versand aus kirchlichen Fach-anwendungen (klick to mail)<br>• Terminanfragen aus kirchlichen Fach-anwendungen<br>• Setzen eines Wiedervorlagetermins in einer Fachanwendung erzeugt Aufgabe in der Groupware-Lösung<br>• Rechnungserstellung und -versand direkt aus dem Finanzwesen | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Vermeidung manueller Bearbeitungs-schritte / Automatisierung der Arbeitsschritte bei Nutzern und Nutzerinnen<br>• Arbeiten ohne Medienbrüche<br>• Reduzierung der Programmvielfalt durch Nutzung zentraler Programmfunktionen („E-Mails werden mit dem Mailprogramm versendet“). | • Sicherstellung der Datenkompatibilität<br>• Erhöhter Administrationsaufwand in der IT | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.12. Zugriff auf SPAM-Mails

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Moderne E-Mail-Systeme sind in der Lage, E-Mails aufgrund ihres Inhaltes oder des Absenders als Spam (unerwünschte Werbung) zu klassifizieren. Damit wird erreicht, dass für den Nutzer/die Nutzerin erkennbar wird, welche E-Mails potentiell unerwünscht sind.<br><br>Auch wenn diese Technik schon sehr ausgereift ist, ist sie sicher nicht immer vollkommen fehlerfrei. Damit der Mensch als Herr über die Technik in der Lage ist hier korrigierend einzugreifen, hat er die Möglichkeit auch E-Mails zu lesen, die durch den Spam-Filter als Spam qualifiziert wurden und nicht im Posteingang liegen. | • Benutzung von Ausschlusswörtern in der Betreffzeile<br>• Vergessen einer Betreffzeile | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • Rückverfolgung und Wiederherstellung versehentlich als SPAM identifizierter und damit aus dem Postfach entfernter E-Mails<br>• Lernender E-Mail-Filter<br>• Höhere Treffergenauigkeit<br>• Kein Verlust von E-Mails | • Beachten von Sicherheitsstandards in der Nutzung und Übertragung von Nachrichten<br>• Gefahr der ungewollten Infizierung der IT Infrastruktur mit Schadprogrammen.<br>• E-Mails werden als Spam qualifiziert, damit überlesen; Gefahr von Informationsverlust<br>• Automatischer Report an Nutzende und Absender<br>• Whitelisting möglich<br>• Die Zulassung einer privaten Nutzung von dienstlichen E-Mailadressen ist eine besondere Herausforderung. Sie schränkt in erheblichem Maße Kontroll- und Protokollierungsmöglichkeiten seitens der IT ein. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.13. Erweiterbarkeit / Attributisierung Adressbuch

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Erweiterbarkeit / Attributisierung des Adressbuchs beschreibt die Möglichkeit, Kontaktdaten aus anderen Quellen zu integrieren.<br><br>Haupt- und ehrenamtliche Mitarbeitende wünschen häufig eine Kommunikation auf unterschiedlichen Wegen, je nach Funktion und Gremium. | | • dienstliche Rufnummer oder Postadresse eines Ehrenamtlichen für die Arbeit im Jugendausschuss |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Erreichbarkeit<br>• Nutzerfreundlichkeit | | • Sicherstellung des Datenschutzes |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.14. Filesharing

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | | **Beispiele** |
| Filesharing beschreibt das direkte Weitergeben von Dateien zwischen zwei oder mehreren Mitarbeitenden der EKIR. Die Dateien liegen dabei entweder auf dem Computer eines/-r Mitarbeiter/-in oder auf einem sogenannten dezidiertem Server. Es besteht die Möglichkeit, die Dateien herunterzuladen und zu bearbeiten oder direkt auf der Serverplattform zu bearbeiten. Jede/r Bearbeiter/-in sieht in der Dateihistorie die unterschiedlichen Bearbeitungsstände der Datei. Insbesondere Dropbox und andere Plattformen sind häufig genutzte Anwendungen für das Teilen und gemeinsame Bearbeiten von Daten und Dokumenten. | | • Inhalte einer Tagesordnung einer Presbytersitzung kann von allen Teilnehmern nicht nur gelesen, sondern auch verändert werden |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Gemeinsames Bearbeiten von Dokumenten<br>• Immer den aktuellsten Bearbeitungsstand auf einen Blick<br>• Rückgriff auf ältere Versionsstände<br>• Zuordnung der Veränderung auf die Bearbeiter und damit direktes Feedback möglich | | • Erhöhter Administrationsaufwand<br>• Eindeutige Rechtevergabe (Lesen, Erstellen, Verändern)<br>• Standardisierte Verhaltensregel im Bearbeiten bzw. Verändern von Dokumenten<br>• Ungewollte Bearbeitungsfreigaben an Unbeteiligte und/oder Unbefugte |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.15. Instant-Messaging-Anwendungen

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Das Instand Messaging beschreibt einen unmittelbaren Kommunikationskanal. Die EKIR Mitarbeiter/-innen hätten die Möglichkeit einer textbasierten Unterhaltung. Zusätzlich zur reinen textbasierten Kommunikation besteht ebenfalls die Möglichkeit, Dateien in Form von Dokumenten, Audio- oder Videoformaten zu übertragen. Zudem kann jede/-r EKIR Mitarbeiter/-in durch eine Statusmeldung signalisieren, ob sie/er aktuell zu erreichen, beschäftigt oder abwesend ist. | | • Pfarrer bietet Gemeindechat als Diskussionsplattform an |
| Begründung/Nutzen | | Konsequenz/Risiko |
| • Schneller und unkomplizierter Austausch<br>• Sichtbarkeit, ob der Adressat erreichbar ist oder nicht<br>• kann Abläufe und Kommunikationsprozesse effektiver machen<br>• unterstützt die Zusammenarbeit in größeren Teams<br>• Integrationsmöglichkeit in andere Plattformen, wie soziale Netzwerke | | • Erhöhte Sicherheitsanforderungen an die IT Infrastruktur<br>• Steigende Anforderung an die IT Infrastruktur durch größeren Datentransfer<br>• Standardisierte Verhaltensregel im Umgang und bei der Benutzung von Instant Messaging |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.16. integrierte Fax Funktion (evtl. via Drittanbieter)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Faxfunktion beschreibt die Möglichkeit, Faxe direkt auf dem Computer zu empfangen bzw. zu versenden. EKIR Mitarbeitende können die Nachrichtenfunktion des E-Mailprogramms zu m Erstellen von Faxnachrichten verwenden, ohne den Arbeitsplatz zu verlassen. Die E-Mailadresse des/der Empfängers/in wird durch die Faxnummer ersetzt. | | • Pfarrer verschickt Faxbestätigung über seinen E-Mail Account |
| Begründung/Nutzen | | Konsequenz/Risiko |
| • Kosten und Zeitersparnis<br>• Umweltschutzaspekt durch Papiereinsparung<br>• Zentralisierung des Nachrichteneingangs<br>• Kein Medienbruch<br>• Kein Stau vor dem Faxgerät | | • Höherer Supportaufwand<br>• Standardisierte Verhaltensregel im Umgang und bei der Benutzung der Faxlösung<br>• Ein möglicher Faxclient soll auf allen gängigen Client-Plattformen laufen und ggfs. Browserbasiert sein. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.17. Multiendgeräte-Fähigkeit (Autosync…)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Multiendgeräte-Fähigkeit beschreibt die Möglichkeit, Mobiltelefone und Tablet PCs mit der Groupware zu verbinden und die Inhalte der Funktionen zu synchronisieren. Hierbei können E-Mails, Adressbücher, Kontakte und Aufgaben auf allen genutzten Endgeräten synchron gehalten werden. Somit haben die Mitarbeiter/-innen der EKiR immer den gleichen und aktuellen Informationsstand auf allen genutzten Geräten. | | • Pfarrerin gleicht ihr Adressbuch mit ihrem privaten iPhone ab<br>• Terminsynchronisierung zwischen iPad und Notebook des Presbyters |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Gleicher Datenstand und Aktualität auf den genutzten Endgeräten des/der Mitarbeiters/-in<br>• Nutzerfreundlichkeit | | • Ggf. höherer Support und Administrationsaufwand<br>• Fehleranfälligkeit<br>• Kompatibilitätsproblem<br>• Ggf. höhere Sicherheitsanforderung an die IT Infrastruktur<br>• Regelung zur dienstlichen Nutzung privater Endgeräte und private Nutzung dienstlicher Geräte zwingend erforderlich<br>• Erhöhte Anforderungen an die IT-Sicherheit durch gemischte Nutzung und Sicherheitslücken von Apps<br>• Erhöhter Aufwand, wenn verschiedene mobile Betriebssysteme unterstützt werden sollen (IOS, Android, RIM) |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.18. Volltextsuche / Indexierung inkl. Attachements

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Volltextsuche bietet die Möglichkeit, den kompletten E-Mail- oder Kontaktbereich nach eingegebenen Schlagworten zu durchsuchen. Die Funktion stellt dann die Suchergebnisse in einer übersichtlichen Ergebnisliste zusammen. Zusätzlich können auch angehängte Dokumente durchsucht werden. Die Indexierung beschreibt die Tätigkeit, ein Dokument bzw. Inhalt mit geeigneten Schlagwörtern zu suchen. Diese Indexierung kann frei oder kontrolliert, d.h. über ein vorbestimmtes Vokabular erfolgen. | | • Pfarrerin gibt über die Volltextsuche der E-Mail die Adresse eines Gemeindemitglieds ein und dieses listet den kompletten E-Mailverkehr der zurückliegenden zwölf Monate auf |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Schnelle Möglichkeit des Filterns von E-Mail -Inhalten<br>• Leichteres Wiederfinden von Dokumenten<br>• Nutzerfreundlichkeit | | • Verlängerte Suchzeiten durch Einbeziehung der E-Mail-Anhänge |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 2.19. Massenmailings

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Massenmailings beschreiben das Verschicken von Informationen und Daten an einen möglichst großen Empfängerkreis. Dabei besteht die Möglichkeit, die Empfängeradressen sichtbar für alle anderen Empfänger/-innen über die CC Leiste oder anonym über die BCC Leiste zu verschicken. Spezialisierte Programme können dabei unterstützen, einen maximalen Personenkreis zu erreichen und trotzdem individuell anzusprechen. | | • Infomail über öffentliche Kirchentreffen<br>• Programmverteilung bspw. zu Oster- oder Weihnachtsfeierlichkeiten |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Informationsbereitstellung an maximale Anzahl von Empfängern/-innen | | • Festlegung, welche Inhalte gestreut werden können<br>• Festlegung, wer Inhalte verteilen darf und wer nicht<br>• Limits für maximale Adressatenanzahl<br>• Ausschluss von Adressaten für bestimmte Inhalte<br>• Verhinderung von Massenmailings hinsichtlich vertraulicher und schützenswerter Inhalte<br>• Gesetzliche Anforderungen beachten (OPT-IN & OPT-OUT)<br>• Messung der Reichweite<br>• Mailings vom E-Mail-System technisch trennen<br>• Gefahr von Blacklisting<br>• Anhäufung von ungenutzten oder nutzlosen Inhalten<br>• Im schlimmsten Fall Weitergabe von vertraulichen und schützenswerten Informationen an unbeteiligte bzw. unbefugte Empfänger/innen |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Soll |

## 2.20. Aufgaben

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Aufgaben beschreiben die Möglichkeit, mittels der Groupwarelösung Aufgaben für sich selbst oder andere zu erstellen. Die Aufgaben können an eine oder mehrere Personen verteilt und zugewiesen werden. Darüber hinaus besteht die Möglichkeit, die Aufgaben für sich selbst oder für die Empfänger zu priorisieren. | | • Arbeitsanweisung an das Sekretariat<br>• Organisation von Veranstaltungen |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Zuweisung von Aufgaben mit Informationen über Priorisierung und Dauer<br>• Festlegung von Nutzer-, Lese- und Bearbeitungsrechten<br>• Schnelle, ortsunabhängige Zuweisung von Arbeitsanweisungen<br>• Anhängen von detaillierten Aufgabenbeschreibungen<br>• Sichtbarkeit des Erledigungsgrades und der Zuständigkeit<br>• Verschickung von Statusberichten<br>• Erstellung von Serientypen<br>• Persönliche Kategorisierung und Nachverfolgung<br>• Erinnerungsmöglichkeit | | • Standardisierte Verhaltensregeln für das Versenden und die Zuweisung von Aufgaben<br>• Ungewollte Weitergabe von vertraulichen Inhalten an Unbeteiligte oder Unbefugte |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Kann |

## 2.21. Integration von Voice-Mail

| Version 0.9 vom 04.06.2013 | |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Voice-Mail ist ein Anrufbeantworter des Telefons. Die Integration von Voice-Mail beschreibt die Möglichkeit, das E-Mail Programm direkt mit dem Telefon zu verbinden. Nachrichten können über den Mediaplayer oder ein Telefon wiedergegeben werden. Ebenso besteht die Möglichkeit, Audionachrichten zu transkribieren und somit als Textnachricht auszugeben. In diesem Fall besteht bei bekannten Kontaktinformationen des/der Absenders/-in die Möglichkeit, mittels E-Mail zu antworten. Übertragene Telefonnummern können direkt in die eigenen Kontakte übernommen werden. Die EKIR-Mitarbeitenden haben somit die Möglichkeit, via Mobiltelefon oder Festnetz auf ihre E-Mails, Voice-Mails, Kontakte und Kalenderdaten zurückzugreifen. Ebenso können Abwesenheitsmitteilungen erstellt und bereitgestellt werden. Voice-Mailboxen können ebenso Faxe entgegennehmen und speichern. | • Pfarrer ruft Voicemail mit seinem Smartphone ab und antwortet den Anrufern via E-Mail |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Nutzende können kommunizieren und zusammenarbeiten, ohne E-Mailprogramm oder andere Anwendungen zu verlassen<br>• Verfügbarkeit wird direkt angezeigt<br>• Direkter Wechsel von E-Mail zu Telefon<br>• Geringere Kosten durch Konsolidierung von Telefonie-, Voicemail- und E-Mail-Systemen | • Höherer Supportaufwand<br>• Standardisierte Verhaltensregel im Umgang und bei der Benutzung von Voice-Mail-Lösungen insbesondere bei der Benutzung von privaten Endgeräten wie Smartphones<br>• Standardisierte IT Infrastruktur<br>• Probleme (Vertraulichkeit / Datenschutz) bei Stellvertretung und Weiterleitung beachten.<br>• Eine bidirektionale Umsetzung stellt hohe technische Anforderungen an ein zentrales |

| | | |
|---|---|---|
| • Vereinfachte Bereitstellung und Verwaltung; dieser Nutzen ist nur in einer standardisierten IT Infrastruktur möglich | Mailsystem, da ein zentrales Voicegateway notwendig wird. Hier sind hohe Sicherheitsanforderungen zu beachten (Seelsorge).<br>• Die Realisierung einer unidirektionalen Umsetzung (Voicemails und Faxe an Mailadresse) ist deutlich einfacher zu realisieren. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Kann |

## 2.22. Private Nutzung

| Version 0.9 vom 04.06.2013 | |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die private Nutzung der Groupware beschreibt die Möglichkeit, für die EKIR-Mitarbeitenden den vollen oder teilweisen Umfang der Groupwarefunktionen für private Belange zu nutzen.<br><br>Die private Nutzung dienstlicher Infrastruktur wird einerseits als mitarbeiterfreundlich gewertet, bereitet bei der Umsetzung aber Probleme in der Administration. Überlässt die EKiR ihren Mitarbeitenden die private Nutzung des E-Mailzugangs, so wird sie zum geschäftsmäßigen Anbieter von Telekommunikationsdiensten. Die Folge ist, dass die EKiR das sogenannte Fernmeldegeheimnis wahren muss. D.h. jegliche Überwachung und Protokollierung des E-Mail-Inhaltes sowie der Verbindungsdaten ist unzulässig. Dieser Umstand macht es äußerst schwierig, praktikable Regelungen zu treffen hinsichtlich SPAM Schutz, Rückverfolgung von Fehlern. Darüber hinaus kommt es zur Verletzung des Datenschutzes bei der Einrichtung von Vertretungen im Abwesenheitsfall der Mitarbeitenden. | • Senden und Empfangen von E-Mails mit privaten Inhalten und Ablage in als privat markierten Ordnern<br><br>• Erstellen und Kennzeichnung von privaten Terminen im Kalender<br><br>• E-Mail an die Familie, dass man länger im Büro bleibt |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Mögliche positive Auswirkung auf die Motivation der Mitarbeiter/-innen<br>• Sichtbarkeit der Vereinbarkeit von privaten und dienstlichen Terminen | • Trennt die EKiR die private E-Mailnutzung nicht logisch oder physisch von der dienstlichen Nutzung, z.B. durch separate E-Mail-Anschriften oder Vorgabe einer Pflicht zur Kennzeichnung als „privat“, so ist de facto jede Kommunikation als privat anzusehen. |

| | |
|---|---|
| | • Störung und/oder Unterbrechung von internen Tätigkeiten<br>• Ablenkung<br>• Standardisierte Verhaltensregel im Umgang und bei Benutzung<br>• Erhöhte Anforderungen an die Infrastruktur durch höhere Datenmenge<br>• Sicherheitsrisiko durch empfangene Schadprogramme<br>• Erhebliche Einschränkungen hinsichtlich von Sicherheitsstandards<br>• Einschränkung der Protokollierung von E-Mail-Verkehr, Zustimmung zu einer vollständigen Protokollierung notwendig.<br>• Dienstliche Belange müssen vorrangig sein. |

| | offene Inhalte | vertrauliche/schützenswerte Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Kann | Kann |

## 2.23. Stellvertreterfunktion

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Stellvertreterfunktion bietet die Möglichkeit, einem/r anderen Nutzer/in der Groupwarelösung Zugriff auf alle oder ausgewählte Funktionen (E-Mail, Kalender, Aufgaben etc.) des eigenen Groupwarezugangs zu gewähren. Der/die Nutzer/in legt hierbei fest, ob der/die Stellvertreter/in über Lese-, Bearbeitungs- oder Löschrechte verfügt. Vordefinierte Berechtigungsprofile vereinfachen die Rechtevergabe. | • Mitarbeiterin im Meldewesen gibt einem Kollegen Lese- und Bearbeitungsrechte für ihr E-Mail-Postfach |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Schnelles Reagieren auf dringliche E-Mails oder Terminanfragen | • Ungewollte Freigabe von Bereichen, die der Vertraulichkeit unterliegen in Unkenntnis über Freigabefunktionen<br>• Standardisierte Vorgehensweise in der |

| | | |
|---|---|---|
| | Einrichtung der Stellvertreterfunktion<br>• Eine Aktivierung soll bei ungeplanter Abwesenheit zentral erfolgen können.<br>• Organisatorische Anforderungen beachten | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Kann |

## 2.24. Integration von Social Network Funktionen

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | | **Beispiele** |
| Die Integration von Social Network Funktionen beschreibt die Möglichkeit, Nachrichten-, Kontakt-, Kalenderfunktionen der Groupwarelösung mit einem oder mehreren Sozialen Netzwerken zu verbinden. Ein/e EKIR Mitarbeiter/in hat so die Möglichkeit, die Kontaktinformationen aus den benutzten sozialen Netzwerken mit der Groupware abzugleichen.<br><br>Social Network Funktionen bedeuten parallel einen Zielkonflikt bei einer sauberen Trennung von dienstlichen und privaten Angelegenheiten. Die Risiken betreffen vor allem die IT Sicherheit und den Datenschutz. Insbesondere der laxe Umgang einer Plattform mit deutschen Datenschutzrichtlinien ist hierbei ein Problem. | | • Übernahme der Facebook Kontakte in eigenes Adressbuch<br>• Kalenderabgleich mit GooglePlus Konto |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Einbeziehung eines größeren Kontaktkreises<br>• Gleichzeitiges Teilen von Informationen in mehreren Leserkreisen<br>• Nachrichten aus den sozialen Netzwerken landen direkt im Posteingang | | • Erhöhte Sicherheitsanforderungen an die IT Infrastruktur<br>• Höherer Supportaufwand<br>• Standardisierte Verhaltensregel im Umgang und Benutzung von Groupware und Sozialen Netzwerken, bspw. Abgleich von Kontakten |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | nicht relevant |

## 3. Gesetzliche Anforderungen

### 3.1. Sicherheitsrichtlinien zur Nutzung von E-Mail

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Eine Sicherheitsrichtlinie zur Nutzung von E-Mail muss erstellt, umgesetzt und den Mitarbeitenden bekannt gemacht werden. Dabei sind die Vorgaben des BSI Grundschutzkataloges anzuwenden. Die Richtlinie muss Regelungen zu den folgenden Aspekten beinhalten:<br>• Festlegen, welche Informationen an wen per E-Mail gesendet werden<br>• Vertretungsregeln für E-Mailpostfächer<br>• Festlegen des Schutzbedarfes bestimmter Daten und Informationen<br>• Festlegen, wann eine Absicherung (Verschlüsselung) der E-Mail bei einem bestimmten Schutzbedarf vorgenommen werden muss | | Das hier vorliegende Dokument stellt eine so genannte Sicherheitsrichtlinie mit Anforderungen für E-Mail-Nutzung dar. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Eine Übersicht aller umzusetzenden Anforderungen wird eindeutig formuliert und kann somit allen Mitarbeitenden bekannt gemacht werden. | | Die Richtlinien müssen jedem beteiligten Mitarbeitenden bekannt gemacht werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 3.2. Trennung Dienstliche und Privatgeräte

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Es ist den Mitarbeitenden in der Regel nicht gestattet, dienstliche Geräte auch privat zu nutzen. Das Nutzen von privaten Geräten für die dienstlichen Belange ist bei der Beachtung der folgenden Maßnahmen erlaubt:<br>• Bei der Nutzung privater Geräte für dienstliche Zwecke gelten die gleichen Sicherheitsregeln, wie bei der Nutzung von dienstlichen Geräten.<br>• Die Speicherung von kirchlichen, personenbezogenen Daten (z.B. Seelsorgeinhalten, Gehaltsabrechnungen d. Mitarbeitende) ist auf den privaten Geräten nicht gestattet. Dies gilt insbesondere für kirchliche Adressbücher, die mit zusätzlichen Informationen verknüpft sind. | | Der Pfarrer einer Gemeinde nutzt sein privates Smartphone aus Bequemlichkeit auch im dienstlichen Umfeld. Dabei hat er sein Outlook-Adressbuch exportiert, um es auf das Smartphone zu importieren. Es ist dem Pfarrer nicht erlaubt, diese Datei per E-Mail unverschlüsselt auf sein Smartphone zu übertragen. Sollten zudem weitere persönliche Informationen wie Termine zur wöchentlichen Lebensberatung oder ähnliches mit den Adressdaten verknüpft sein, so ist das Smartphone besonders bzw. genauso wie das dienstliche IT-System, zu schützen (mindestens mit einer Tastensperre und Code). |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Durch das ungeregelte Nutzen privater IT-Systeme kann es zu schwerwiegenden Verletzungen der Vertraulichkeit kommen. Zudem sind private Geräte nicht entsprechend der Sicherheitsrichtlinien sicher konfiguriert, sodass Schwachstellen nicht bekämpft werden können. | | Wird die Nutzung privater Geräte / E-Mail erschwert oder eingeschränkt, so kann es zu Leistungseinbußen von kirchlicher Arbeit besonders bei ehrenamtlichen Mitarbeitenden kommen, da sie lieb gewonnene eigene IT-Systeme nicht mehr oder nur eingeschränkt benutzen. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 4. Non-Funktionale Anforderungen

### 4.1. Mehrere Corporate Designs / Domainen

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Multi-Domain beschreibt die Möglichkeit, mehrere Webseiten auf dem gleichen Hostingpaket zu betreiben. Es besteht so die Möglichkeit, dass ein/e Mitarbeiter/in der EKiR verschiedene E-Mail Adressen hat, diese aber alle in einem Postfach zusammenlaufen. | | • Individuelles Erscheinungsbild der einzelnen Gemeinden der EKIR |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Hoher Individualisierungsgrad<br>• Vielzahl von Kontaktmöglichkeiten | | • Höherer Pflegeaufwand<br>• Einheitliches Gesamtbild sofern gewünscht geht verloren |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

### 4.2. (Nicht)-Weiterleitungen vertraulicher Mails

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Vertrauliche E-Mails dürfen nicht an Dritte weitergeleitet werden. Dazu muss der entsprechende Text immer auf Vertraulichkeit geprüft werden, bevor eine manuelle Weiterleitung der E-Mail vorgenommen wird. Automatische Umleitungen von E-Mail-Postfächern dürfen nicht aktiviert werden.<br><br>Bei der zunehmenden Mobilität wird zunehmend gewünscht, immer und von beliebigen Orten aus auf E-Mail zugreifen zu können. Ein Mechanismus hierfür ist die automatische Weiterleitung von E-Mails. Es wird daher empfohlen, E-Mails nicht automatisiert weiterzuleiten. | | Es besteht ein Vertrauensverhältnis zwischen dem Pfarrer der Gemeinde und einem Gemeindeglied. Aufgrund einer Frage des Gemeindegliedes in einer E-Mail, leitet der Pfarrer diese Frage weiter. Er entfernt aber die vorherigen vertraulichen Textpassagen. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Vertraulichkeit ist ein Schutzziel und muss auch in E-Mails umgesetzt werden.<br><br>Durch unbedacht eingerichtete Weiterleitungen besteht die Gefahr des Daten- bzw. Vertraulichkeitsverlustes. Dies kann dann vorkommen, wenn E-Mails unerwartet vertrauliche Mitteilungen enthalten. | | Die Mitarbeitenden müssen für Vertraulichkeit sensibilisiert werden.<br><br>Deaktivierung der automatischen Weiterleitung<br><br>Manuelle Löschung schutzwürdiger Inhalte<br><br>Technische Maßnahmen notwendig (z.B. ein Weiterleitungsverbot an externe Systeme bei Kennzeichnung "vertraulich"). |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Muss |

### 4.3. Account-Nutzung: Wer bekommt Groupware-Funktionen zu welchen Konditionen?

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Jede Groupwarelösung bietet eine Vielzahl von Funktionen und Anwendungen. Je nach Umfang des zur Verfügung gestellten Leistungspaketes berechnet sich der Preis pro Nutzendem. Jeder Personenkreis der EKIR hat ggf. unterschiedliche Anforderungsbedürfnisse an die Groupwarelösung. Je nach Bedürfnissen kann man maßgeschneiderte Pakete anbieten. | | • Voller Funktionsumfang für Mitarbeitende des Landeskirchenamtes in Düsseldorf<br>• Grundfunktionen wie E-Mail, Kalender, Aufgaben und Kontakte für die Presbyter |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Beachtung der Wirtschaftlichkeit<br>• Kosteneinsparung | | • Hoher Differenzierungsgrad in der Bereitstellung für die Nutzenden<br>• höherer Support- und Administrationsaufwand |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 4.4. Anzahl Empfänger

| | | | Version 0.9 vom 04.06.2013 |
|---|---|---|---|
| **Beschreibung** | | **Beispiele** | |
| Die Anzahl der Empfänger beschreibt die maximale Anzahl der Adressaten einer E-Mail, eines Termins oder einer Aufgabe. So kann bei Limitierung der Empfängeranzahl gesteuert werden, dass nur autorisierte Mitarbeitende bspw. Massenmailings durchführen dürfen. | | Maximal fünf Empfänger für EKIR Mitarbeitende aus der Verwaltung; bei größeren Empfängergruppen erfordert es die Zustimmung einer weisungsbefugten Person | |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** | |
| • Verhinderung von Massenmails<br>• Empfänger werden nicht mit möglicherweise nicht relevanten Infos versorgt<br>• Disziplinierung der Nutzenden hinsichtlich Versendevorgaben von E-Mails | | • Nichtverschicken einer E-Mail bei Überschreitung<br>• Zu starke Beschränkung kann zu Unzufriedenheit der Nutzenden führen<br>• ggf. höherer Supportaufwand | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** | |
| **Verbindlichkeitsgrad** | Soll | Soll | |

### 4.5. Dateianhanggröße

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Die Dateianhanggröße beschreibt die maximale Größe, die ein/eine Anwender/in der Groupware an eine zu verschickende E-Mail anhängen kann. Fotos und Videos sind i.d.R. die größten Dateianhänge | | • Versand von Fotos oder Videos von Gemeindegliedern von der Kindstaufe an ihren Pfarrer |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Verhinderung von langen Up- und Down-loadzeiten bei der Beschränkung von Anhanggrößen<br>• Mögliche Kostenreduzierung durch kleine Bandbreiten der beauftragten Serviceprovider<br>• Disziplinierung der Nutzenden | | • Nichtverschicken einer E-Mail bei Überschreitung der Anhanggröße<br>• E-Mails mit großen Dateianhängen können nicht empfangen werden<br>• Zu starke Beschränkung kann zu Unzufriedenheit der Nutzer führen<br>• Ggf. höherer Supportaufwand |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

### 4.6. Historie in Kalender

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| In der Kalenderhistorie werden gelöschte oder geänderte Einladungen, Terminanfragen oder Termine vermerkt. So hat man die Möglichkeit in der Vergangenheit liegende Termine bzw. Informationen zu Terminen/Einladungen wiederaufzurufen und ggf. wiederherzustellen. | | • Pfarrer hat versehentlich eine Terminanfrage gelöscht, obwohl er eigentlich zustimmen wollte; er hat die Möglichkeit, in der Kalenderhistorie diesen Termin wiederherzustellen und wie gewünscht zuzustimmen. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Wiederherstellung von Terminen oder Einladungen<br>• Nutzerfreundlichkeit | | • Höhere Anforderungen an Speicherplatz<br>• Ggf. höherer Administrations- und Supportaufwand |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 4.7. Höchste Verfügbarkeitsanforderungen

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Fähigkeit eines IT Service oder eines identifizierbaren Teils eines IT Service, bei Bedarf die vereinbarte Funktion auszuführen. Die Verfügbarkeit wird durch Aspekte in Bezug auf Zuverlässigkeit, Wartbarkeit, Servicefähigkeit, Performance und Sicherheit bestimmt. Die Verfügbarkeit wird in der Regel als Prozentwert ausgedrückt, der häufig basierend auf der vereinbarten Servicezeit und der Ausfallzeit berechnet wird. Die Verfügbarkeit wird mithilfe von Messgrößen aus dem Geschäftsergebnis des IT Service berechnet (garantierte Verfügbarkeit in Prozent gleich 100–Ausfallzeiten×100 Servicestunden). Gemessen wird über ein definiertes Zeitintervall, welches im SLA festzulegen ist. | | Die Seelsorge-E-Mail Adresse sollte sich durch eine ständige Erreichbarkeit auszeichnen |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| • Ständige Verfügbarkeit der Groupwarefunktionen für alle Arbeitsfelder und Aufgaben der EKIR | | • Höchste Anforderung an Support und Administration |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 4.8. Postfachgröße

| | | |
|---|---|---|
| | | **Version 0.9 vom 04.06.2013** |
| **Beschreibung** | **Beispiele** | |
| Die Postfachgröße beschreibt die maximale Anzahl der darin enthalten E-Mails und/oder die maximal speicherbare Dateigröße. Fotos und Videos haben i.d.R. die größten Datenmengen und damit kann die maximale Postfachgröße schnell erreicht sein. Die Anforderung verlangt eine bedarfsgerechte Festlegung der Postfachgröße. | • Idealerweise unbegrenzter Speicher für Pfarrer/-innen damit auch Fotos und Videodateien der Gemeindeglieder empfangen werden können im Sinne einer kompletten Gemeindearbeit<br>• Begrenzung im Verwaltungsbereich um als vorbeugende Maßnahme den Austausch von Belanglosen Anhängen bspw. Spaßvideos einzuschränken | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| • limitierter Speicher fördert die Nutzerdis-ziplin hinsichtlich des Posteingangs<br>• unbegrenzter Speicher wird i.d.R. Anwenderfreundlicher wahrgenommen | • Schnelle Kapazitätserreichung bei großen Dateianhängen<br>• Höhere Reife in der Benutzung der Groupwarelösung<br>• Pflegeaufwand an das eigene Postfach<br>• Durchführung einer automatischen Archivierung zur Reduktion der Postfachgröße (nach Funktionen / Bedeutung) und ggfs. Datenvorhaltung auf wirtschaftlicherem Speichermedium (z.B. Transfer von SSD auf SATA-Storage). | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 5. Sicherheitsanforderungen

### 5.1. Authentizität

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Durch eine eindeutige Zuweisung von persönlichen E-Mailpostfächern und dem Implementieren von Authentisierungsmechanismen (z.B. mit geheimen Passwörtern, die nur dem/der Inhaber/in dieses Postfaches bekannt sind) kann die Urheberschaft und Zugehörigkeit zur versendeten E-Mail im Normalfall sichergestellt werden.<br><br>Wenn an die Authentizität einer Nachricht höhere Sicherheitsanforderungen gestellt werden, so kann durch eine digitale Signatur der Nachricht zusätzlich die Echtheit des/der Verfassers/in nachgewiesen werden. | | Im Falle einer Vertretung gibt die Sekretärin ihr persönliches Passwort nicht an die Vertretung weiter, da persönliche Postfächer nur eindeutig von der zugewiesenen Person benutzt werden dürfen. Es wäre in diesem Fall nicht mehr sicher nachvollziehbar, wer tatsächlich die E-Mail von diesem Postfach versendet hätte. (Sekretärin oder Vertretung).<br><br>Eine 2-Faktor-Authentisierung kann bei einem Notebook eines wichtigen kirchlichen Vertreters notwendig sein. Dazu erhält er neben einem Passwort noch ein Sicherheitstoken (z.B. einen USB-Stick), der bei der Anmeldung an das Notebook eingesteckt werden muss. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Der/die Absender/in einer E-Mail kann somit zu einem hohen Grade immer festgestellt werden.<br><br>Der E-Mailverkehr wird effizienter und die Nachvollziehbarkeit das Vertrauen in das Medium nimmt zu. | | Sollten bisher persönliche E-Mail-Postfächer oder andere Goupware-Accounts von mehreren Personen genutzt werden, dann müssen diese Regelungen auf Anwendung regelmäßig überprüft werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.2. Identität und Authentisierung

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Für den Zugriff auf E-Mails und das Versenden von E-Mails bezüglich eines Postfaches mit hohem Schutzbedarf ist ein ausreichend starker Mechanismus mit 2-Faktor-Authentisierung zur Erbringung des Nachweises der Identität einzurichten. | | Eine 2-Faktor-Authentisierung kann bei einem Notebook eines wichtigen kirchlichen Vertreters notwendig sein. Dazu erhält er neben einem Passwort noch ein Sicherheitstoken (z.B. einen USB-Stick, ein digitales Zertifikat), der bei der Anmeldung an das Notebook eingesteckt werden muss. Durch das Erlangen eines Authentisierungsfaktors kann sich ein Angreifer noch nicht die berechtigte Identität verschaffen. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Durch eine 2-Faktor-Authentisierung ist es schwer möglich, eine unberechtigte Authentisierung durchzuführen, da das Erlangen beider Authentisierungsfaktoren (Geheimnisse) bedeutend unwahrscheinlicher ist. | | Eine Analyse und die Auswahl einer/der Lösung(en) für die 2-Faktor-Authentisierung muss vorgenommen werden. Zudem ist mit erhöhtem Beschaffungs- und Supportaufkommen zu rechnen, da meist ein zusätzliches Gerät oder Zertifikat erstellt und im Verlustfalle neu ausgestellt werden muss. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.3. Betriebsordnung (Einweisung der Benutzer von E-Mail)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | **Beispiele** | |
| Alle Nutzenden müssen im Umgang mit dem E-Mail- bzw. Groupware-Client geschult werden. Neben der reinen Nutzung der Client-Software ist es jedoch auch notwendig, den Nutzenden die grundlegende Funktionsweise des Groupware-Systems zu erläutern. Den Nutzenden muss insbesondere vermittelt werden, welche Sicherheitsmechanismen ihnen zur Verfügung stehen, so dass sie in der Lage sind, diese korrekt und sinnvoll einzusetzen. | Dies könnte z.B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein ungewöhnliches Verhalten der Kommunikationssoftware gemeldet werden soll. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| Bei der Sicherheit kommt es oft auf jedes Glied in der Kette an, damit Sicherheit auch umgesetzt ist. Die beste technische Sicherheitsmaßnahme nützt nichts, wenn der bedienende Mensch sie mit oder ohne Absicht umgeht. | Die Mitarbeitenden müssen für die sichere Anwendung von E-Mail und Groupware informiert und sensibilisiert werden. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.4. Black-Liste-Verfahren (Ausschluss von Teilnahme)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Sollte ein/e Mitarbeitende/r oder eine kirchenfremde Person über ein E-Mailpostfach wiederholt und nach Ermahnung unerwünschte E-Mails versenden, Massen-E-Mails oder E-Mails, die gegen Kirchenrecht verstoßen, versenden, so kann er/sie auf Antrag vom regulären E-Mail-Verkehr ausgeschlossen werden. Dies wird durch das sogenannte Black-Listing-Verfahren umgesetzt. Sollte das Postfach zentral von einer Kirchenstelle betrieben werden, so kann die Erlaubnis der Nutzung entzogen werden. | | Ein ehrenamtlicher Mitarbeiter schickt wiederholt Kettenbriefe mit anstößigem Inhalt an eine große Anzahl von kirchlichen E-Mail-Adressen. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Das Black-List-Verfahren erleichtert den Umgang mit unerwünschten E-Mails enorm. | | Um zu verhindern, dass irrtümliche Sperrungen wieder aufgehoben werden, muss ein solches Verfahren zentral verantwortet werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.5. Eingangskontrolle Gateway (Viren, SPAM, Trojaner, Pishing, Hoaxes, Würmer, DDoS-Angriffe und Bot-Netze)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Bei der Anwendung eines Web-Mail-Dienstes (wie z.B. Gmail oder GMX) muss die Anti-Virenfunktion in den Einstellungen aktiviert werden. Zudem ist auf dem kirchlichen PC, Notebook oder sonstigem Client eine automatische Schadcode-Prüfung (Virenscan) der E-Mails durchzuführen.<br><br>Alle Virenscanner müssen regelmäßig, am besten automatisch, mit neuen Signaturen aktualisiert werden. | | Der Gemeinde-PC im Sekretariat hat einen aktuellen Virenscanner installiert und aktiviert. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Wenn der Einfall von Schadcode minimiert werden kann, so werden viele potentielle Gefährdungen minimiert. | | Der Einsatz von Antivirensoftware muss flächendeckend umgesetzt und geprüft werden.<br><br>Eine Software-Lösung für alle kirchlichen Stellen sollte zur Verfügung gestellt werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.6. Einsatz eines E-Mail-Scanners auf dem Mailserver (Viren, Spam, Content, Compliance)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Alle beteiligten internen E-Mailserver der EKiR müssen eine Eingangskontrolle der E-Mails vornehmen. Dazu werden E-Mails automatisch auf Schadcode gefiltert. | | Der verantwortliche E-Mail-Server der EKiR filtert alle E-Mails mit Anhängen, die Schadcode enthalten (wie z.B. Viren, SPAM, Trojaner, Pishing, Hoaxes, Würmer, DDoS-Angriffe und Bot-Netze). |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Ein Großteil der externen Bedrohungen für IT-Systeme resultiert aus Schadcode, der in E-Mails übertragen wird. | | Entsprechendes Know-how muss bereitgestellt werden. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.7. Regelung zur Nutzung von Massenmail-Verteilern

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| E-Mails können an eine Vielzahl von Empfängern/Empfängerinnen gleichzeitig ohne großen Aufwand versendet werden. Damit die Postfächer nicht sinnlos mit Massen-E-Mails überhäuft werden, muss es Einschränkungen in der Nutzung dieses Dienstes geben. Dazu gehört es, das nicht alle Mitarbeitende Zugriff auf E-Mail-Verteiler haben. Nur die Personen, die aufgrund ihrer kirchlichen Aufgaben diese Funktion benötigen sollen eine solche Berechtigung erhalten. Alle anderen müssen technisch oder auch organisatorisch davon ausgeschlossen werden.<br><br>Zudem sollte jede/-r Benutzer/-in die Weitergabe seiner/ihrer E-Mail-Adresse auf das Nötigste einschränken, um sich vor Massenmails zu schützen.<br><br>Generell sollte regelmäßig überprüft werden, ob die in einer Mailingliste diskutierten Inhalte das Lesen lohnen, sonst ist sie abzubestellen. | Ein Mitarbeitender ist sehr aktiv im Internet auf Foren und sozialen Netzwerken unterwegs und gibt überall seine E-Mail-Adresse bekannt. Daraufhin wird er mit Werbung überhäuft und kann seine wichtige E-Mail-Post nicht mehr vollständig bearbeiten.<br><br>Ein nichts ahnender Mitarbeiter schickt unbeabsichtigt eine private Nachricht ausversehen an einen großen E-Mail-Verteiler und veröffentlicht so geheime Informationen. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Die Minimierung von Massen-E-Mails kann die Nutzung der E-Mailkommunikation massiv erleichtern, da Postfächer weniger überfüllt sind. Zudem wird das Auffinden wichtiger E-Mails erleichtert. | Es müssen Maßnahmen zur Kontrolle der Einhaltung dieser Anforderung durchgeführt werden. Dazu gehört es, E-Mail-Verteiler von Verantwortlichen verwalten zu lassen und auch die Berechtigungen zu dokumentieren. Die Berechtigungen müssen auch regelmäßig überprüft werden, damit |

| | | |
|---|---|---|
| | | kein ungehindertes Anwachsen der Berechtigungen die Maßnahme unwirksam macht. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.8. Sichere Administration des E-Mail-Systems

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Ein Mailserver ist so zu konfigurieren, dass er nicht zur Verbreitung von Spam missbraucht werden kann. Dafür sollte der Mailserver so konfiguriert sein, dass er E-Mails nur für die eigene Organisation entgegennimmt und nur E-Mails verschickt, die von Mitarbeitern der Organisation stammen. Alle anderen E-Mails sollten mit einer Fehlermeldung abgewiesen werden.<br><br>Es ist ebenso zu vermeiden, dass Non Delivery Notifications aufgrund falscher Empfängeradressen erzeugt werden. Vielmehr ist dafür zu sorgen, dass E-Mails, für die die Institution nicht zuständig ist, gar nicht erst angenommen werden.<br><br>Folgende Maßnahmen müssen zum Schutz ergriffen werden:<br><br>• Schon als Spam klassifizierte E-Mails dürfen nicht automatisch beantwortet oder weitergeleitet werden.<br>• Die Absenderadresse der Antwort bzw. Weiterleitung muss eine Adresse aus dem Namensraum der Institution sein. Der Absender der eingehenden E-Mail darf nicht verwendet werden. | Der Abwesenheitsassistent ist so eingestellt, dass nur einmalig eine Abwesenheitsbenachrichtigung geschickt wird.<br><br>Wenn eine kirchliche Stelle keinen eigenen Mailserver betreibt, sondern über einen oder mehrere Mail-Clients direkt auf den Mailserver eines Providers zugreift, sollte mit dem Provider abgeklärt werden, welche Regelungen dort gelten und welche Sicherheitsmaßnahmen ergriffen worden sind. |

| | |
|---|---|
| • Es muss verhindert werden, dass ein bestimmtes Ziel (Zieladresse oder Zieldomain) unkontrolliert mit einer großen Anzahl von E-Mails beschickt wird.<br><br>Die Aktivitäten auf dem Mailserver müssen regelmäßig protokolliert und diese Protokollierungen regelmäßig ausgewertet werden. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Ein kirchlicher E-Mail-Server kann nach Umsetzung nicht als Spam-Verteiler genutzt werden.<br><br>Unerwünschte E-Mails, vor allem Spam-Mails stören das produktive Arbeiten. | Administratoren müssen ausreichend geschult sein und die Anforderungen umsetzen. |

| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
|---|---|---|
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.9. Sichere Installation des E-Mail-Systems

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Alle für den Betrieb des Groupware-Systems benötigten Komponenten müssen sicher installiert und konfiguriert werden. Dazu müssen die folgenden Aspekte betrachtet werden:<br><br>• Die Bausteine der IT-Grundschutz-Kataloge geben Vorgaben zur sicheren Installation, die bei der Installation umgesetzt werden sollten.<br>• Während der Installation müssen wichtige Authentisierungsdaten eingestellt werden. Es ist darauf zu achten, dass dabei sichere Passwörter gewählt werden.<br>• Der Zugriff auf die Installationsquellen ist mit Mitteln des Betriebssystems so abzusichern, dass nur berechtigte Administratoren darauf zugreifen können.<br>• Entsprechend der Planung der Systemlandschaft müssen die für den Betrieb des Groupware-Systems benötigten Komponenten (z. B. auch die Sicherheitsgateways) installiert und konfiguriert werden.<br>• Ungenutzte Komponenten müssen, soweit es geht, von der Installation ausgeschlossen oder | |

| | | |
|---|---|---|
| später deaktiviert werden. | | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| Die sichere Installation ist die Basis für einen sicheren Betrieb. | Geeignete Installationsmedien sollten möglichst zentral bereitgestellt werden. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.10. Sichere Konfiguration der E-Mail-Clients

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Bei der Konfiguration der Groupware-Clients sollten die folgenden Punkte berücksichtigt werden:<br><br>• Eine sichere Vorkonfiguration durch die Administratoren muss durchgeführt werden<br>• E-Mail-Programme sollten so eingestellt sein, dass sie aktive Inhalte in HTML-formatierten E-Mails nicht ohne Rückfrage ausführen.<br>• Wegen der möglichen Gefahren durch HTML-formatierte E-Mails sollten keine HTML-formatierten E-Mails verschickt werden.<br>• Das Betriebssystem bzw. der E-Mail-Client sollte so eingerichtet sein, dass Dateien zunächst nur in Viewern oder anderen Darstellungsprogrammen angezeigt werden, die eventuell in den Dateien enthaltene Programmcodes, wie Makros oder Skripte, nicht ausführen.<br>• Die Vorschau-Funktion im E-Mailprogramm sollte deaktiviert sein. | Die Benutzer sollten darüber informiert werden, dass sie E-Mail-Filterregeln selbst konfigurieren können. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Die sichere Konfiguration ist für einen sicheren Betrieb wesentlich. | Die Nutzenden müssen darauf hingewiesen werden, dass sie die Basis-Konfiguration nicht selbsttätig ändern dürfen. |

| | offene Inhalte | vertrauliche/schützenswerte Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Muss |

## 5.11. Umgang mit unerwünschten E-Mails (Spam)

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Alle kirchlichen Stellen behalten sich das Recht vor, bestimmte E-Mail-Inhalte zu Filtern und somit mit Schadcode infizierte E-Mails oder andere ungewollten Werbe-Emails zu isolieren und aus dem System auszuschließen.<br><br>Mögliche Maßnahmen gegen unerwünschte E-Mails sind die folgenden:<br><br>• Es sollte genau überlegt werden, ob und welche E-Mail-Adressen auf Webseiten bekannt gegeben werden. Hierfür können beispielsweise aufgabenbezogene E-Mail-Adressen eingerichtet werden<br>• Mitarbeitende dürfen auf keinen Fall auf unerwünschte E-Mails reagiert werden.<br>• Gegen akute Belästigung durch Spam ist die Benachrichtigung des eigenen Mailproviders sowie des Mailproviders des Verursachers, damit diese gegen den Verursacher vorgehen können vorzunehmen. | Eine Filterung der E-Mails findet bereits auf dem Mail-Server statt.<br><br>Um sich vor unerwünschten E-Mails zu schützen, sollte jede/-r Benutzer/-in die Weitergabe seiner/ihrer E-Mail-Adresse auf das Nötigste einschränken.<br><br>Grundsätzlich sollten alle Benutzer Spam ignorieren und löschen. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Unerwünschte E-Mails, welche auch unter dem Begriff "Spam" bekannt sind, werden in Massen verschickt, belästigen die | Es kann vereinzelt vorkommen, dass E-Mails versehentlich als „Spam“ ausgefiltert werden. |

| | | |
|---|---|---|
| Empfänger und stören den laufenden Betrieb der IT-Infrastruktur, angefangen bei den E-Mail-übertragenden Systemen bis zu den Clients der Benutzer. | | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.12. Verschlüsselung der Datenhaltung

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Sollte ein Web-Speicherplatz genutzt werden auf dem personenbezogene Daten gespeichert werden, so muss die Ablage in verschlüsselter Form vorgenommen werden. Als Web-Speicherplatz (oder auch Online-Festplatte) wird Speicherplatz bei Internet-Anbietern bezeichnet.<br><br>Kunden erhalten diesen Online-Speicherplatz von einem Web-Anbieter zugeteilt, um Dateien längerfristig zu speichern und einfach über das Internet auf die Daten zugreifen zu können. Vor allem mobile Mitarbeiter schätzen diese Möglichkeit, da sie von beliebigen Standorten schnell und uneingeschränkt auf ihre Daten zugreifen können.<br><br>Es sind nur die derzeit als hinreichend sicher geltenden kryptografischen Verfahren entsprechend dem Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (**http://www.bsi.de**) einzusetzen. | Mitarbeitende nutzen externen Web-Speicherplatz, um kircheninterne Daten in einem Internet-Cafe oder bei einer anderen Gemeinde abzurufen. Durch eine unzureichende Absicherung der übertragenen Informationen (sowohl Authentisierungs- als auch Nutzdaten) können anschließend auch Unbefugte auf weitere dort gespeicherte kircheninterne Daten zugreifen. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Bei der unverschlüsselten Datenablage liegt allerdings auch ein großes Risiko, denn der Zugriff auf externe Speichermöglichkeiten macht Datenflüsse schwerer kontrollierbar. | |
| **offene Inhalte** | **vertrauliche/schützenswerte** |

| | | Inhalte |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Muss |

## 5.13. Verteilerregelung (CC, BCC)

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | **Beispiele** | |
| Bei Massen-E-Mails, wie Einladungen an Externe darf nicht CC, sondern BCC benutzt werden. Bei der Eingabe von Adressen bei CC werden alle Empfänger über die anderen E-Mailadressen informiert. Bei der Nutzung von BCC bleiben für die einzelnen Empfänger andere Empfänger verborgen. | Bei der Versendung des Gemeindebriefes einer kleinen Gemeinde per E-Mail werden alle Empfänger in BCC eingetragen. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| Oft ist nicht erwünscht, dass der gesamte Adressatenkreis inklusive E-Mail-Adresse an alle Empfänger gesendet wird. | Die Mitarbeitenden müssen über diesen Sachverhalt informiert bzw. sensibilisiert werden. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss | Muss |

## 5.14. Verschlüsselung des Transports / Datenübertragungsbedingungen

| | Version 0.9 vom 04.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Verschlüsselung und digitale Signaturen dienen dem Schutz der Integrität und Vertraulichkeit sowie auch der Nicht-Abstreitbarkeit elektronisch über-mittelter Nachrichten.<br><br>Ein Konzept für die kryptographische Absicherung von E-Mail muss erstellt werden:<br><br>• Bei der Transport-verschlüsselung ist das TLS/SSL-Verfahren einzusetzen<br>• Protokolle wie SMTP oder LDAP müssen TLS/SSL zur sicheren Kommunikation nutzen.<br>• Es darf nur TLS 1.0 oder höher bzw. SSL 3.0 oder höher eingesetzt werden, da erst ab diesen Versionen eine Server-Authentikation stattfindet.<br>• Die Verschlüsselung zwischen den E-Mailservern ist vorzunehmen. Dies kann mit der SMTP-Protokoll-erweiterung STARTTLS (oportunistic TLS) implementiert werden.<br>• Es sollen von allen beteiligten E-Mailservern Zertifikate gemäß dem X.509-Standard eingesetzt werden. | Bei der Transportverschlüsselung achtet der Administrator oder IT-Verantwortliche darauf, dass in den Einstellungen „TLS 1.0“ im E-Mail-Client aktiviert ist. |

| | |
|---|---|
| • Es sind nur die derzeit als hinreichend sicher geltenden kryptografischen Verfahren entsprechend dem Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (http://www.bsi.de) einzusetzen. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| SSL 2.x sollte hingegen nicht verwendet werden, da diese Versionen keinen Schutz vor "Man-in-the-Middle"-Angriffen bieten. | Beim Einsatz von TLS/SSL ist zu beachten, dass verschlüsselte Daten hinsichtlich aktiver Inhalte und Schadprogramme nicht zentral, also z. B. am Sicherheitsgateway, überprüft werden können. |

| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
|---|---|---|
| **Verbindlichkeitsgrad** | Soll | Muss |

## 5.15. (Nicht-) Weiterleitung vertraulicher E-Mails

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Vertrauliche E-Mails dürfen nicht an Dritte weitergeleitet werden. Dazu muss der entsprechende Text immer auf Vertraulichkeit geprüft werden, bevor eine manuelle Weiterleitung der E-Mail vorgenommen wird. Automatische Umleitungen von E-Mail-Postfächern dürfen nicht aktiviert werden.<br><br>Bei der zunehmenden Mobilität wird zu-nehmend gewünscht, immer und von beliebigen Orten aus auf E-Mail zugreifen zu können. Ein Mechanismus hierfür ist die automatische Weiterleitung von E-Mails. Es wird daher empfohlen, E-Mails nicht automatisiert weiterzuleiten. | | Es besteht ein Vertrauensverhältnis zwischen dem Pfarrer der Gemeinde und einem Gemeindeglied. Aufgrund einer Frage des Gemeindegliedes in einer E-Mail leitet der Pfarrer diese Frage weiter. Er entfernt aber die vorherigen vertraulichen Textpassagen. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Vertraulichkeit ist ein Schutzziel und muss auch in E-Mails umgesetzt werden.<br><br>Durch unbedacht eingerichtete Weiterleitungen besteht die Gefahr des Daten- bzw. Vertraulichkeitsverlustes. Dies kann dann vorkommen, wenn E-Mails unerwartet vertrauliche Mitteilungen enthalten. | | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | nicht relevant | Muss |

## 5.16. Erstellen eines Notfallplans für den Ausfall von E-Mail-Systemen

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Für den Ausfall von E-Mail-Systemen muss ein Notfallplan erstellt werden, worin die folgenden Aspekte betrachtet werden:<br><br>• Systemkonfiguration dokumentieren<br>• Datensicherungskonzept erstellen<br>• Wiederanlaufplan erstellen<br>• Notfallübungen durchführen | | |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Der teilweise oder komplette Ausfall eines Groupware-Systems hat in vielen Fällen gravierende Auswirkungen auf die Arbeitsmöglichkeiten der Benutzer, da alle Server-basierten Aktionen nicht mehr ausgeführt werden können. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten bei einem Ausfall durchzuführen sind. | | Die Notfallplanung für das eingesetzte E-Mail / Groupware-System muss den existierenden Notfallplan der kirchlichen Stelle berücksichtigen. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 5.17. Überwachung und Protokollierung des Mailservers

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Sicherheitsrelevante Ereignisse müssen protokolliert werden. Generell ist bei der Protokollierung Folgendes zu beachten:<br>• Es muss ein Protokollierungskonzept erstellt werden.<br>• Der Zugriff auf die Protokolldaten muss eingeschränkt werden.<br>• Wichtige Systemereignisse wie Änderungen, Fehler und Störungen an Hardware, Betriebssystem, Treibern, Diensten und sonstiger Software sind zu protokollieren und regel-mäßig auszuwerten.<br>• Zugriff auf die Monitoring-Werkzeuge einschränken | | Im Protokollierungskonzept ist festzulegen, welche Protokolldaten im Groupware-System gesammelt und ausgewertet werden sollen.<br><br>Der Zugriff auf die durch das Groupware-System angebotenen Monitoring-Werkzeuge ist auf die berechtigten Administratoren einzuschränken. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Damit die Systemfunktionen und die Systemsicherheit eines Groupware-Systems überwacht werden können, müssen sicherheitsrelevante Ereignisse protokolliert werden. | | Da bei der Protokollierung auch personenbezogene Daten anfallen können, sind der Datenschutzbeauftragte und der Mitarbeitervertretung in die Planung einzubeziehen. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 5.18. Automatische Antwort bei Nichtanwesenheit

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | | **Beispiele** |
| Bei Abwesenheit ist die automatische Antwort bei Nichtanwesenheit so zu konfigurieren, dass diese E-Mail nur einmal gesendet wird.<br><br>Der Text der automatischen Antwort ist daraufhin zu prüfen, ob die Nachricht adäquate Informationen für beliebige Kommunikationspartner enthält.<br><br>Die meisten E-Mail-Programme mit Autoreply-Funktion bieten auch die Möglichkeit, die Benachrichtigung nach Kriterien, die die Benutzer selbst festlegen können, zu steuern.<br><br>Wenn Regeln zur Steuerung von Autoreply-Funktionen eingesetzt werden sollen, sollten die Administratoren dies entsprechend für die Benutzer vorbereiten. | | Es kann beispielsweise voreingestellt werden, dass interne E-Mail-Absender andere Antworten erhalten als externe. |
| **Begründung/Nutzen** | | **Konsequenz/Risiko** |
| Zu viele und eventuell vertrauliche Informationen können ein Sicherheitsrisiko darstellen (z.B. „Alle Mitarbeiter der Gemeinde sind wegen einer Weiterbildung eine Woche nicht in der Gemeinde vor Ort anzutreffen.“). | | Hierfür werden in der Regel aber tiefere Kenntnisse des E-Mail-Clients benötigt. |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll | Soll |

## 5.19. Vereinheitlichung der E-Mail-Adressen

| | | Version 0.9 vom 04.06.2013 |
|---|---|---|
| **Beschreibung** | **Beispiele** | |
| E-Mail-Adressen sollten aufgrund von klaren Namenskonventionen vergeben werden. Wichtig ist, dass keine Nicht-ASCII-Zeichen wie Umlaute innerhalb von E-Mail-Adressen verwendet werden.<br><br>Für wichtige kirchliche Aufgaben sind funktionsbezogene E-Mail-Adressen einzurichten. Durch Urlaub, Dienstreisen, Krankheit oder personelle Veränderungen können zu unterschiedlichen Zeitpunkten aber ganz verschiedene Personen für die Bearbeitung einer E-Mail zuständig sein. Es muss dabei dokumentiert sein, welche organisations- und funktionsbezogenen Adressen existieren und zu welchem Zweck sie dienen. | z.B. das „é“ in notcafé@kichengemeinde.de | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** | |
| Sind in einer E-Mail-Adresse nicht standardkonforme Umlaute oder Zeichen enthalten, so kann die korrekte Weitergabe und eine Erreichbarkeit nicht garantiert werden. | Es müssen Regelungen zur Namenskonvention in der EKiR entwickelt werden.<br><br>Es müssen Regelungen zur Registrierung von Domainnamen geschaffen werden. | |
| | **offene Inhalte** | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Kann | Kann |

## *Anhang – Überblick Verbindlichkeit*

| Anforderungsbereich | Anforderung | offene Informationen | vertraulich/schützenswerte Informationen |
|---|---|---|---|
| Betrieblich | Erreichbarkeit von Mail-Verteiler-Listen | Soll | Soll |
| Funktional | E-Mail | Muss | Muss |
| | Kalender | Muss | Muss |
| | Kontakte | Muss | Muss |
| | Funktionale Postfächer | Muss | Muss |
| | Assistenzfunktion | Muss | Muss |
| | Webmail Zugriff | Muss | Muss |
| | Multiple Domainen | Muss | Muss |
| | Räume und Ausstattungsgegenstände | Soll | Muss |
| | Zugriff auf E-Mail-Archiv | Soll | Soll |
| | Einbinden mehrerer Adressverzeichnisse | Soll | Soll |
| | Anbindung an / von Fachanwendungen | Soll | Soll |
| | Zugriff auf SPAM-Mails | Soll | Soll |
| | Erweiterbarkeit / Attributisierung Adressbuch | Soll | Soll |
| | Filesharing | Soll | Soll |
| | Instant-Messaging-Anwendungen | Soll | Soll |
| | integrierte Fax Funktion | Soll | Soll |
| | Multiendgerät-Fähigkeit | Soll | Soll |
| | Volltextsuche / Indexierung inkl. Attachements | Soll | Soll |
| | Massenmailings | Kann | Soll |
| | Aufgaben | Kann | Kann |
| | Integration von | Kann | Kann |

| Anforderungsbereich | Anforderung | offene Informationen | vertraulich/schützenswerte Informationen |
|---|---|---|---|
| | Voice-Mail | | |
| | Private Nutzung | Kann | Kann |
| | Stellvertreterfunktion | Kann | Kann |
| | Integration von Social Network Funktionen | Kann | nicht relevant |
| Gesetzlich | Sicherheitsrichtlinien zur Nutzung von E-Mail | Soll | Soll |
| | Trennung Dienstliche und Privatgeräte | Soll | Soll |
| Non-funktional | Mehrere Corporate Designs / Domainen | Muss | Muss |
| | (Nicht)-Weiterleitung vertraulicher Mails | Soll | Muss |
| | Account-Nutzung | Soll | Soll |
| | Anzahl Empfänger | Soll | Soll |
| | Dateianhanggröße | Soll | Soll |
| | Historie in Kalender | Soll | Soll |
| | Höchste Verfügbarkeitsanforderungen | Soll | Soll |
| | Postfachgröße | Soll | Soll |
| Sicherheit | Authentizität | Muss | Muss |
| | Identität und Authentisierung | Muss | Muss |
| | Betriebsordnung | Muss | Muss |
| | Black-Liste-Verfahren | Muss | Muss |
| | Eingangskontrolle Gateway | Muss | Muss |
| | Einsatz eines E-Mails-Scanners auf dem Mailserver | Muss | Muss |
| | Regelung zur Nutzung von Massenmail- | Muss | Muss |

| Anforderungsbereich | Anforderung | offene Informationen | vertraulich/schützenswerte Informationen |
|---|---|---|---|
| | Verteilern | | |
| | Sichere Administration des E-Mail-Systems | Muss | Muss |
| | Sichere Installation des E-Mail-Systems | Muss | Muss |
| | Sichere Konfiguration der E-Mail-Clients | Soll | Muss |
| | Umgang mit unerwünschten E-Mails | Muss | Muss |
| | Verschlüsslung der Datenhaltung | Soll | Muss |
| | Verteilerregelung | Muss | Muss |
| | Verschlüsselung des Transports / Datenübertragungsbedingungen | Soll | Muss |
| | (Nicht-) Weiterleitung vertraulicher E-Mails | nicht relevant | Muss |
| | Erstellen eines Notfallplans für den Ausfall von E-Mail-Systemen | Soll | Soll |
| | Überwachung und Protokollierung des Mailservers | Soll | Soll |
| | Automatische Antwort bei Nichtanwesenheit | Soll | Soll |
| | Vereinheitlichung der E-Mail-Adressen | Kann | Kann |

**Anlage 7 c**

Anlage 7 c

# Ergänzende Anforderungsbeschreibung Meldewesen

**Hinweis:**
**Dieses Dokument befindet sich im Entwurfsstadium.**

## Einführung

Das folgende Dokument bietet ihnen eine Übersicht der ergänzenden Anforderungen einer in der Evangelischen Kirche im Rheinland (EKiR) eingesetzten Meldewesensoftware. Eine Meldewesensoftware bildet alle kommunal gelieferten personenbezogenen Daten ab, überträgt diese auf die kirchlichen Strukturen. Es bietet sich die Möglichkeit, die für den kirchlichen Auftrag erforderlichen Informationen aktuell zu erfassen und auszuwerten.

Die ergänzenden Anforderungen für eine Meldewesenlösung bauen direkt auf den Basisanforderungen für IT-Systeme in der EKiR auf (*Dokument: Beschreibung der Basisanforderungen für IT Systeme in der Evangelischen Kirche im Rheinland*). Sie gelten für alle Nutzenden der eingesetzten Meldewesenlösung.

Hinsichtlich des Aufbaus des Baukastensystems der IT-Standards und des Aufbaus dieser Dokumentation sei auf das oben genannte Dokument „Basisanforderungen“ verwiesen.

# *Inhalt*

# 1. Betriebliche Anforderungen

## *1.1. Dienstleistungsvertrag zur Einhaltung der IT Standards*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Ein Dienstleistungsvertag zur Einhaltung der IT Standards beschreibt einen gegenseitigen Vertrag zwischen Auftragnehmer und Auftraggeber. Der Auftragnehmer verpflichtet sich zur Leistung der versprochenen Dienste unter Berücksichtigung und Einhaltung der geltenden IT Standards des Auftraggebers. Der Auftraggeber verpflichtet sich seinerseits zur Entrichtung der vereinbarten Vergütung. | Die EKiR schließt nur einen Vertrag mit einem Anbieter für Meldewesensoftware, der sicherstellt, dass er die in der EKiR geltenden IT Standards vollumfänglich erfüllt. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Einhaltung von IT Standards und damit Wahrung dergeltenden betrieblichen, funktionalen, non-funktionalen, gesetzlichen, kirchenspezifischen und Sicherheitsanforderungen | • Formale Prüfung der Dienstleister durch die EKiR<br>• Eingeschränkte Anbieterseite<br>• Vertrauen auf Transparenz seitens des Softwareanbieters |
| **Verbindlichkeitsgrad** | **vertrauliche/schützenswerte Inhalte**<br>Muss |

## 2. Funktionale Anforderungen

### *2.1. Datenübernahme Einwohnermelderegister*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Datenübernahme Einwohnermelderegister beschreibt, wie oft und in welcher Form die Datenübernahme zwischen den jeweiligen Kommunen und dem Rechenzentrum stattfindet. | Das Rechenzentrum der Kommune Köln schickt wöchentlich den Änderungsdatensatz in elektronischer Form an die Kigst. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Sicherstellung der Aktualität der kommunal erfassten Daten ev. Gemeindeglieder<br>• Sicherstellung § 14 Kirchenmitgliedschaftsgesetz und § 27 Verwaltungsordnung | • Abhängigkeit zur Kommune |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### *2.2. Datenübernahme Kirchengemeinde (kirchlicher Lebenslauf, Gruppenaktivitäten)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Datenübernahme Kirchengemeinde beschreibt die Übernahme der von der Kirchengemeinde erfassten Daten / Aktivitäten im zentralen Melderegister. | Die Kirchengemeinde erfasst die Taufe und die Konfirmation eines Gemeindegliedes im Bestand. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Schnelle und komfortable Auskunftsmöglichkeit für die Kirchengemeinde<br>• Vollständige Weitergabemöglichkeit der Daten bei Wegzug aus der Gemeinde | • Abhängigkeit zum Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.3. *Bereitstellung von Bescheinigungen (Mitgliedschaft, Zuwendungen etc.)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Bereitstellung von Bescheinigungen beschreibt eine Methode der Dienstleistungen für Gemeindeglieder. | Gemeindeglied spendet 200 € für die soziale Arbeit in der Kirchengemeinde, und benötigt für das Finanzamt eine Spendenbescheinigung.<br><br>Ein Gemeindeglied benötigt für die Taufe seines Kindes in einer anderen Kirchengemeinde eine Dimesoriale. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Führung der Spenden nach gesetzlichen Vorgaben | • Abhängigkeit für Datenvollständigkeit zur Kommune |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.4. *Bereitstellung von Wahlunterlagen*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Bereitstellung von Wahlunterlagen dient als Grundlage für die Presbyterwahl. Bereitgestellt werden die Zuordnungen der Regionalstruktur Wahlbezirke, der Ausdruck notwendiger Wahlunterlagen. | Durch die Kirchengemeinde werden die Wahlbezirke festgelegt und im Meldewesen erfasst. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • kostengünstige Möglichkeit, die Presbyterumswahl durchzuführen, da Listen durch Kirchengemeinde selber erstellt und gestaltet werden können<br>• aktuelle Listen am Auslegedatum | • Risiko für unvollständige Wahlunterlagen durch inkonsequente Pflege der Daten, damit verbunden Anfechtbarkeit der Wahl |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.5. *Kirchenbuch*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Kirchenbuch regelt die Führung der Kirchenbücher in digitaler und gesetzlich vorgeschriebener Art und Weise. | Durch den Kirchenbuchführer der Kirchengemeinde wird die Mitarbeiterin beauftragt, alle Amtshandlungen über Mewis-NT im Kirchenbuch zu erfassen. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Schneller Zugriff auf die Kirchenbücher im Auskunftsfall<br>• Erfassung der Daten nur einmal, da eine Übernahme an das Meldewesenprogramm und Ausdruckmöglichkeit für die Meldung an die Kommune | • Risiko für unvollständige Kirchenbücher durch inkonsequente Datenpflege<br>• Abhängigkeit zum Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.6. *Gemeindegliedverzeichnis (Verwaltung der Amtshandlung, Kirchenaustritt)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Gemeindegliederverzeichnis ist Verwaltung aller für die Kirchengemeinde relevanten Daten der Gemeindeglieder. Es dient der Gemeinde als Hilfsmittel in der Verwaltung der Gemeindeglieder. | Die Mitarbeiterin einer Kirchengemeinde holt sich die für eine Bescheinigung notwendigen Informationen aus dem Meldewesenprogramm |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Zentrale Auskunftsmöglichkeit<br>• Schneller Zugriff auf Personendaten | • Abhängigkeiten zur Kommune und zum Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.7. *Abbildung Regionalteil (Verlinkung Adress- und Personendaten)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Der Regionalteil beschreibt die | Durch den zuständigen Kirchenkreis |

| | |
|---|---|
| Grenzen der einzelnen Kirchengemeinde und ordnet die Straßen in die jeweiligen Bezirke ein. | werden neue Straßen dem richtigen Pfarrbezirk zugeordnet. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Sicherstellung der Vollständigkeit der Regionalstruktur | • Abhängigkeiten zur Kommune und zum Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.8. *Abbildung von Gemeindefusionierung und Archivierung der Daten nicht mehr existierender Gemeinden*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Abbildung von Gemeindefusionierungen und Archivierung von Daten aus nicht mehr existierenden Gemeinden dient der Abbildung und Recherche über nicht mehr existierende Gemeinden | Zwei Gemeinden haben vor einigen Jahren fusioniert. Um auch nach einigen Jahren noch erkennen zu können, wie der Ursprung der zwei Gemeinden war, werden die ursprünglichen Daten archiviert. Die Recherche in den „alten Kirchenbüchern“ ist auf diesen Wege einfacher und komfortabler. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Zentrale Auskunftsmöglichkeit auch nach Fusionierung noch möglich | • Abhängigkeit zu Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.9. *Übernahme von Daten aus Fremdsystemen (KIRA, DAVIP Online)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Übernahmen von Daten aus Fremdsystemen beschreiben den Weg der vollständigen Datenweitergabe eines Gemeindegliedes beim Wohnortwechsel. | Ein Gemeindeglied zieht von Hamburg nach Bonn, die in Hamburg gesammelten Informationen (Amtshandlungsdaten) werden an die neue Kirchengemeinde übermittelt. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Vollständiges Bild des kirchlichen Lebenslaufs auch nach Umzug in eine andere Stadt | • Abhängigkeit zu Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.10. *Statistische Auswertung sowohl im kirchlichen Auftrag (Gemeindearbeit) als auch für den Regionalteil*

| Version 0.9 vom 21.06.2013 |
|---|

| Beschreibung | Beispiele |
| --- | --- |
| Statistische Auswertung ist ein wichtiges Hilfsmittel zur Feststellung statistischer Auswertungen in der Gemeindearbeit. | Für die Errichtung eines Kindergartens in einer Kirchengemeinde wird eine Altersstatistik benötigt, diese kann aus dem Programm erstellt werden. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Einfaches Hilfsmittel, um die Entwicklung der Kirchengemeinde festzustellen | • Abhängigkeit der vollständigen Datenübermittlung durch die Kommune |
| **Verbindlichkeitsgrad** | **vertrauliche/schützenswerte Inhalte** |
| | Muss |

### 2.11. *Importschnittstelle für regionale Daten*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Importschnittstelle für regionale Daten beschreibt die Möglichkeit der Datenübernahme von neuen Regionaldaten der Kommune. | Die Kommune ändert für einen gesamten Stadtteil die Straßennamen. Anhand der dazugehörigen Schlüssel kann über diese Schnittstelle ein Datenabgleich erfolgen |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Regionaldaten sind immer auf dem aktuellen Stand der Kommune | • Abhängigkeit zur Kommune |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.12. *Auslesen von CSV Daten (Etikettendruck)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Das Auslesen von CSV-Daten dient als Hilfsmittel zur weiteren Datenverarbeitung in einem anderen Programm (Excel, Word, Access). | Für die Erstellung eines Serienbriefes werden die Daten einer bestimmten Gruppe in eine csv-Datei exportiert und in Word weiterverarbeitet. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Schnelle und unkomplizierte Weiterverarbeitung von Daten | • Nach Export der Daten ggf. kein ausreichender Schutz mehr nach Datenschutzgesetz |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.13. *Pflege von Besuchs- und Verteilerbezirken*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Pflege von Besuchs- und Verteilerbezirken ist das Werkzeug für die aktive Gemeindearbeit einer Kirchengemeinde | Eine Kirchengemeinde richtet Besuchsbezirke für Ihre Kirchengemeinde ein und erstellt für den/die ehrenamtliche/n Mitarbeiter/in regelmäßig eine aktuelle Liste; so kann der |

| | |
|---|---|
| | ehrenamtliche Mitarbeiter immer auch die neuen Zuzüge in seinem Bezirk besuchen |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Besuchsbezirkslisten und Verteilerlisten können bei Bedarf ausgedruckt werden und sind immer auf dem aktuellen Stand | • Abhängigkeit zu Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.14. *Flexible Personen(-kreis)suche / Recherchemöglichkeiten*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die flexible Personensuche bietet der Kirchengemeinde die Möglichkeit der Suche nach aktiven Gemeindegliedern und deren Angehörigen auf unterschiedlichste Art und Weise. | Die Mitarbeiterin sucht ein Gemeindeglied. Sie weiß zwar das Geburtsdatum und die Straße, in der es gemeldet ist, nicht jedoch, wie der genaue Nachname lautet. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Flexible Suchfunktion auch bei unvollständigen Daten<br>• Unkomplizierte und schnelle Bereinigung des Bestandes durch Kontrolle | • Abhängigkeiten zu Kommune und Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.15. *Inner- und zwischenkirchlicher Datenaustausch (IKIDA und ZWIKIDA)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Der innerkirchliche und zwischenkirchliche Datenaustausch stellt die Übermittlung der kirchlichen Amtshandlungsdaten eines Gemeindegliedes innerhalb der Landeskirche und Landeskirchenübergreifend sicher. | Daten eines Gemeindegliedes werden beim Umzug innerhalb des Bereiches der Landeskirche mitgegeben. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • genaue Auskunftsmöglichkeiten auch nach Umzug in eine neue Gemeinde<br>• Weitergabe kirchlicher Lebenslauf | • Abhängigkeit von der Richtigkeit der Daten aus der ehemaligen Gemeinde |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.16. *Datentransfer an die Kommune (Wegzug, Austritt, Tod)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Datentransfer an die Kommune | Daten werden in den |

| | |
|---|---|
| beschreibt den Weg der erfassten Amtshandlung von der Kirchengemeinde an die Kommune, gesammelt über das Rechenzentrum | Kirchengemeinden über das Kirchenbuch erfasst, an Mewis-NT weiter gegeben und dann gesammelt über das Rechenzentrum an die Kommune übermittelt |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Keine Papiermeldungen mehr an die Kirchengemeinde<br>• Garantierte Erfassung durch digitalen Weg | • Abhängigkeit zum Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll |

### 2.17. *Anzeige von aktiven und inaktiven Datensätzen*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Anzeige von aktiven und inaktiven Datensätze n beschreibt den Vorgang der Historie innerhalb eines Datensatzes. | Ein ehemaliges Gemeindeglied ist aus der Kirche ausgetreten, durch den Austritt wechselt das Gemeindeglied sofort nach Übermittlung durch die Kommune bzw. nach Erfassung des Austrittes durch die Kirchengemeinde in den inaktiven Datenbestand. So ist sichergestellt, dass die Daten erhalten bleiben, die Person aber nicht mehr aktiv am Gemeindeleben teilnimmt |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Genauere Recherchemöglichkeiten | • Abhängigkeit zum Programm |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.22. *Browsergestützter Client*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Aufgrund der gesetzlichen Vorgaben muss den meldewesenverarbeitenden Stellen ein sicherer Client zur Verfügung gestellt werden. | Das Programm wird als geschützte Browseranwendung über eine geschützte Leitung (z. B.VPN) zur Verfügung gestellt. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Einhaltung der gesetzlichen Vorgaben<br>• Sicherheit für Gemeindegliederdaten ist gewährleistet | • Abhängigkeit zum Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.23. *Export von Kirchbüchern via pdf.File*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Der Export in eine pdf-Datei | Kirchengemeinde liest die Daten aus |

| | |
|---|---|
| unterstützt die Möglichkeit, schnell und kostengünstig die Kirchbücher nach den gesetzlichen Vorgaben auszudrucken und vorzuhalten. | den Kirchenbüchern aus, druckt diese selber aus und hebt diese als lose Blattsammlung auf. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Kein Rätselraten mehr bei undeutlich geschriebenen Einträgen<br>• Keine doppelte Erfassung mehr, da Daten per Knopfdruck an das Meldewesen gesendet werden können | • Abhängigkeit vom Rechenzentrum |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.24. *Ausweisung von inkonsistenten Datensätzen*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Anweisung von inkonsistenten Datensätzen beschreibt die Vorgehensweise bei durch die Kommune fehlerhaft gelieferten Daten. | Personen, die z.B. einen doppelten Hauptwohnsitz haben, können mit Mewis für Mehrfachwohnsitz ausgewertet werden. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Zugriff auf die Personendaten, auch wenn diese fehlerhaft durch die Kommune übermittelt wurden | • Abhängigkeit zur Kommune |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.25. *Serienbrieferstellung*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Hier wird die Möglichkeit über eine csv-Datei (Quelle) geschaffen, dass Gemeinden Anschreiben mit wenig Aufwand gestalten können. | Gemeinde liest die Adressdaten eines Besucherkreises aus, damit dieser durch die Ehrenamtlichen besucht werden kann. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Weiterbearbeitung der Daten in einem anderen Programm möglich | • Genaue Einhaltung des Datenschutzes wichtig<br>• Daten können durch nicht zuverlässigen Umgang an Dritte gelangen |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.26. *Nichtauswertbarkeit Sperrvermerk (Gefahr für Leib- und Leben, Adoption)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Nichtauswertbarkeit bei Sperrvermerken beschreibt die gesetzlich vorgegebenen Sicherheitsmerkmale für Personen | Ein Richter und seine Familie haben einen Sperrvermerk für Leib und Leben. |

| mit Sperrvermerken. | |
|---|---|
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Erhalt der Daten auch bei besonders schutzwürdigen Personen | • Durch unzuverlässigen Umgang mit Daten können diese an unbefugte Dritte gelangen<br>• Genaue Einhaltung der gesetzlichen Vorgaben notwendig |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.27. *Datenweitergabe an die Einwohnermelderegister*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Datenweitergabe beschreibt den automatischen Austausch aller mitgliedschaftsbegründeten Amtshandlungen von der Kirchengemeinde zur Kommune. | Taufmeldung aus der Kirchengemeinde wird im Mewis NT erfasst und zentral über das Rechenzentrum an die zuständige Kommune weitergeleitet. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Sicherstellung, dass mitgliedschaftsbegründete Amtshandlungen an die Kommune weitergeleitet werden<br>• Fehlerminimierung im Meldebestand<br>• Gesicherte und verfügbarkeitsunabhängige Weiterleitung<br>• Zeitersparnis | • Keine telefonische Auskunftsbereitschaft<br>• Abhängigkeit von der Verfügbarkeit der IT Services |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 2.28. *Datenexport*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Der Datenexport dient als Schnittstelle für verschiedene Fachabteilungen. | Für die Erhebung der Gemeindegliederzahlen benötigt das Landeskirchenamt die Zahlen jeder Kirchengemeinde. Durch die Schnittstelle des Datenexports können die Daten direkt in die Fachanwendung übernommen werden. EKD-Tabelle 2 |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| •schnelle Weiterbearbeitung von Daten | •Abhängig von Kommunen, Rechenzentrum und Kirchengemeinde<br>•Gefährdung des Datenschutzes |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

## 3. Gesetzliche Anforderungen

### *3.1. Berücksichtigung des Kirchenmitgliedschaftsgesetzes (RS 10) § 17*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Das verwendete Programm muss den erforderlichen Datenaustausch zwischen den Gliedkirchen gewährleisten. Die Gliedkirchen sind verpflichtet, ein einheitliches Programm der Datenverarbeitung für die Daten der Kirchenmitglieder zu entwickeln oder den automatischen Datenträgeraustausch auf andere Weise sicherzustellen. | Das eingesetzte Programm muss die ZWIKIDA (zwischenkirchlicher Datenaustausch) und die IKIDA (innerkirchlicher Datenaustausch) Schnittstellen unterstützen. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • 10 Kirchenmitgliedschaftgesetz § 17 | • |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### *3.2. Berücksichtigung der Verwaltungsordnung (RS 400) § 60 KVO*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Für jede Kirchengemeinde ist ein Verzeichnis der Kirchenmitglieder und deren Familienangehöriger (Gemeindegliederverzeichnis) nach den hierfür geltenden Bestimmungen zu führen. | Das Gemeindegliederverzeichnis beinhaltet die personenbezogenen Daten der Kirchenmitglieder mit ihren Familienangehörigen (Familienverbund). |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • 400.1 Verwaltungsordnung § 60 KVO | • |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### *3.3. Berücksichtigung der Verordnung über das Gemeindegliederverzeichnis (RS 13)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Das Gemeindegliederverzeichnis muss vorsehen, dass folgende personenbezogene Daten der Kirchenmitglieder und ihrer Familienangehörigen (Ehepartnerin oder –partner, Lebenspartnerin oder -partner einer eingetragenen Lebenspartnerschaft, minderjährige leibliche, Stief- und Pflegekinder, leibliche Stief- und Pflegeeltern minderjähriger Kinder sowie deren minderjährige Geschwister) aufgenommen werden können.<br>Bei den Datenfeldern wird nach folgenden Kategorien unterschieden:<br>• Kirchenmitglied<br>• Familienangehörige des Kirchenmitgliedes<br>• Kirchliche Daten des Kirchenmitgliedes<br>Kirchliche Daten der Familienangehörigen des Kirchenmitgliedes, die nicht derselben oder keiner öffentlich-rechtlichen Religionsgemeinschaft angehören | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • 13 Verordnung über die in das Gemeindeverzeichnis aufzunehmenden Daten der Kirchenmitglieder mit ihren Familienangehörigen. | • |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 3.4. Berücksichtigung der Kirchenbuchordnung (RS 410) § 5

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Nicht in der Wohnsitzkirchengemeinde vollzogene Amtshandlungen sind innerhalb der Evangelischen Kirche in Deutschland der Wohnsitzkirchengemeinde mitzuteilen.<br><br>Die kirchenbuchführenden Stellen sind verpflichtet, die sich aus den Kirchenbüchern ergebenden Daten über Taufen, Konfirmationen, Trauungen und Bestattungen sowie die Daten über Aufnahmen und Austritte von Kirchenmitgliedern umgehend der Stelle mitzuteilen, die das Gemeindegliederverzeichnis führt.<br><br>Liegt für einen katholischen Ehepartner bei der Trauung ein Dispens vor, sind die Daten über die Trauung der katholischen Kirche mitzuteilen.<br><br>Mitgliedschaftsbegründende Amtshandlungen (Taufe und Aufnahme) sind der für den Wohnsitz zuständigen Meldebehörde zur Fortschreibung des Melderegisters und der zuständigen Kirchensteuerverteilungsstelle mitzuteilen.<br><br>Zuständig für die Mitteilungen ist die kirchenbuchführende Stelle der Kirchengemeinde, in deren Zuständigkeitsbereich die Amtshandlung vollzogen worden ist. | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |

| | |
|---|---|
| • 410 Kirchenbuchordnung § 5 | • |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 3.5. *Berücksichtigung des Kirchengesetzes zur Regelung des Meldewesens (RS 435) §§ 1 und 3*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Es ist ein einheitliches Meldewesen in der EKiR durch eine zentrale Datenverwaltung zu nutzen, um den innerkirchlichen und den zwischenkirchlichen Datenaustausch sicherzustellen. Im Gemeindegliederverzeichnis werden die personenbezogenen Daten der Kirchenmitglieder mit ihren Familienangehörigen erfasst, die nach der Verordnung über die in das Gemeindegliederverzeichnis aufzunehmenden Daten der Kirchenmitglieder mit ihren Familienangehörigen in der jeweils geltenden Fassung aufzunehmen sind.<br><br>Weitere Daten, insbesondere Aufzeichnung persönlicher oder seelsorglicher Art, die in Wahrnehmung des Seelsorgeauftrages bekannt geworden sind, dürfen nicht in das Gemeindegliederverzeichnis aufgenommen werden. | Alle Gemeinden benutzen ein einheitliches Programm mit einer gemeinsamen mandantenfähigen Datenhaltung, um den elektronischen Datenaustausch zu gewährleisten. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • 435 Kirchengesetz zur Regelung des Meldewesens § 1 und 3 | • |
| **Verbindlichkeitsgrad** | **vertrauliche/schützenswerte Inhalte** |
| | Muss |

### 3.6. *Berücksichtigung der kommunalen Meldegesetze*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Meldebehörde darf einer öffentlich-rechtlichen Religionsgemeinschaft zur Erfüllung ihrer Aufgaben Daten ihrer Mitglieder übermitteln. Die übermittelten Daten dürfen ausschließlich für seelsorgerische und steuerliche Zwecke verwendet werden. Eine Datenübermittlung ist nur dann zulässig, wenn sichergestellt ist, dass bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen sind. Die Feststellung hierüber trifft das Innenministerium.<br><br>Für das Meldegesetz Hessen gilt außerdem:<br>Die öffentlich-rechtliche Religionsgemeinschaft teilt dem für das Meldewesen zuständig Ministerium die getroffenen Datenschutzmaßnahmen mit. | Über ein IT-Sicherheitskonzept muss die Einhaltung der Datenschutzmaßnahmen sichergestellt werden. Das gilt nicht nur für das benutze Meldewesenprogramm, sondern für den kompletten IT-Verbund, d.h. vom Benutzer über den lokalen PC, die Internetverbindung, das Programm und die Datenbank. Es muss verhindert werden, dass die Daten unkontrolliert extrahiert werden und auf nicht geschützten Datenträgern verbleiben. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Meldegesetz NRW, Rheinlandpfalz, Saarland und Hessen § 32 | • Die Meldebehörde stoppt die Datenlieferung an die EKiR. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 3.7. *Grundgesetz (Art. 4)*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Freiheit des Glaubens, des Gewissens und die Freiheit des religiösen und weltanschaulichen Bekenntnisses sind unverletzlich. Die ungestörte Religionsausübung wird gewährleistet. | |

| Begründung/Nutzen | Konsequenz/Risiko |
| --- | --- |
| • | • |
| | vertrauliche/schützenswerte Inhalte |
| Verbindlichkeitsgrad | Muss |

### *3.8. Datenschutzverordnung unter Berücksichtigung der staatlichen Regelungen*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| | |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### *3.9. geklärte Verfahrensverantwortung*

| | Version 0.9 vom 21.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| | |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| | |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

# 5. Non-Funktionale Anforderungen

## *5.1. Herstellersupport*

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Alle Hersteller von Softwareprodukten bieten den Anwendern einen Support an. Die Art und Weise der Bereitstellung kann auf verschiedenen Wegen erfolgen, bspw. FAQs auf der Webseite des Herstellers, Online Formulare, E-Mail, telefonische Service oder Fernwartung. Der Herstellersupport fungiert i.d.R. als Second- oder Thirdlevel Support. | • KIGST Kundensupport per Fernwartung mittels Hilfsprogramm |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Hersteller hat das umfangreichste Know-how über Funktionen und technische Voraussetzungen der Software<br>• Sicherstellung der Nutzbarkeit der Software über SLAs möglich<br>• Nutzerfreundlichkeit | • Sicherstellung des Datenschutzes<br>• mögliche Mehrkosten durch Verträge |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 5.2. *intuitive Benutzeroberfläche*

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die intuitive Benutzeroberfläche bezeichnet die vom Nutzer erlebte Qualität in der Bedienbarkeit einer Softwarelösung. Benutzerfreundlich ist hierbei insbesondere eine einfache, selbsterklärende, zum Benutzenden und den Aufgaben passende Bedienung. | • Sekretärin in der Pfarrei erstellt ohne Anwendersupport vollständige Listen zur Presbyterwahl |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Nutzerfreundlichkeit<br>• Übersichtlichkeit<br>• Kostenersparnis durch Wegfall von Supportnutzung | • Gebrauchstauglichkeit der Softwarelösung |
| **Verbindlichkeitsgrad** | **vertrauliche/schützenswerte Inhalte** |
| | Muss |

# 6. Sicherheitsanforderungen

## *6.1. Prozess des IT-Sicherheitsmanagements [ISMS] (Standard)*

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die heute vorhandenen Sicherheitskonzepte und -maßnahmen sind i.d.R. Insellösungen oder Ad-Hoc-Maßnahmen mit unterschiedlichem Sicherheitsniveau. Hieraus ergibt sich eine latente Bedrohung für die Handlungsfähigkeit und das Image der EKiR. Hinzu kommen oftmals hohe Abhängigkeiten vom Know-how einzelner Zulieferer oder Mitarbeiter. | Ein Katastrophenfall im Bereich MW führt zu der Frage „Wer ist hier verantwortlich?“ und damit zu einer grundsätzlichen Kompetenzdiskussion.<br>Liegt die Verantwortung bei der Kirchenleitung, dem IT-Leiter der EKiR oder den jeweiligen MW-Sachbearbeitenden als Verfahrensinhaber? Die Angst vor persönlichen Konsequenzen könnte eine solche Diskussion dominieren. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Angesichts der sich mit hohem Tempo weiter entwickelnden Bedrohung der IT-Sicherheit wachsen sowohl die Anforderungen an das Wissen und die Fähigkeiten präventiver und reaktiver Sicherheitsmaßnahmen, als auch die Erwartung, die Verantwortung für den Schutz der Informationen und den sicheren Betrieb der Technik ganzheitlich zu betrachten und zu steuern. | Der Einsatz von Informationstechnologie ist unmittelbar mit der Rolle und Verantwortung eines IT-Sicherheitsbeauftragten zu verknüpfen.<br>Der/die Sicherheitsbeauftragte initiiert den Aufbau und die Aktualisierung einer IT-Sicherheits-organisation in der EKiR. Der/die Sicherheitsbeauftragte erstellt und stimmt die Ziele der Informationssicherheit der EKiR ab. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 6.2. Sicherer Verfahrensbetrieb (Standard) und gesicherte Betriebsumgebung

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Der sichere Verfahrensbetrieb betrachtet den abgesicherten Betrieb aller zur Benutzung des Verfahrens benötigten Betriebselemente, insbesondere Server/ Client/ Übertragung, Rechenzentrumsbetrieb, Applikationsbetrieb. Abgesicherter Betrieb bedeutet die Einhaltung der elementaren Schutzziele des BSIGrundschutzkataloges und die Beachtung der BSI-Standards 100-1 bis 100-4 innerhalb des IT-Verbundes. | Nachdem immer wieder Lastspitzen auf dem Webserver für das MW auftauchen und das System für die Nutzer über Tage nicht funktionsfähig ist, ergibt eine Analyse, dass eine anonyme Organisation tausende Anfragen pro Minute an die Webserver zum Betrieb der MW-Applikation gesendet (DDOS) und diesen schlicht überfordert hat. Eine unzureichende Systemkonfiguration hat dies nicht verhindert. Aufgefallen war dies bisher nicht. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Ein sicherer Verfahrensbetrieb setzt die Betrachtung aller eingesetzten Komponenten auf allen Ebenen voraus (s. 6.1.) Eine fortlaufende Auditierung sowie die kontinuierliche Anpassung aller Betriebselemente stellt dies sicher. Dieser Prozess endet erst mit der Einstellung des beschriebenen Verfahrens (Betriebsende). | Der sicherere Verfahrensbetrieb setzt eine kontinuierliche Betrachtung und Anpassung aller eingesetzten Betriebselemente voraus. Es muss die Regel "Alles, was nicht ausdrücklich erlaubt ist, ist verboten" realisiert sein. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 6.3. Datensicherung im Rechenzentrum

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Das Datensicherungs-Konzept beschreibt, welche Inhalte zu sichern sind, in welchen Zeitabständen eine Datensicherung durchgeführt wird, in welcher Art und Weise die Datensicherung zu erfolgen hat, zu welchem Zeitpunkt die Datensicherung durchgeführt wird. Das Datensicherungs-Konzept ist elementarer Bestandteil der Katastrophenvorsorge. | Nach einem Blitzeinschlag am Freitag unmittelbar neben dem Rechenzentrum sind Server und Festplatten beschädigt. Nach dem Einspielen der letzten Datensicherung vom vergangenen Samstag sind Eingaben und Anpassungen von fünf Werktagen und 2000 Nutzern verloren. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Die Pflicht zur Datensicherung und zur Archivierung von kirchlichen Meldedaten/ Kirchbüchern ergibt sich aus den gesetzlichen Vorschriften. Von der kurzzeitigen Aufbewahrung (begrenzt auf einen Tag bis drei oder auch sechs Monate) unterscheidet sich die längerfristige Datenarchivierung, die anderen Gesetzmäßigkeiten unterliegt. Datenverluste könnten existenzbedrohend sein. | Ebenso sind im Rahmen der elektronischen Archivierung die gesetzlichen Anforderungen einzuhalten (Kirchbuch). Eine langfristige Archivierung in geeigneter Art und Weise ist durchzuführen. Das Datensicherungskonzept muss für die Gewährleistung einer funktionierenden Datensicherung die Datenrestaurierbarkeit mittels praktischer Übungen als Verpflichtung vorsehen. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 6.4. Benutzeraktivitätsprotokoll

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| IT-Systeme und Anwendungen bieten Funktionalitäten an, um die Nutzung der Operationen, ihre Reihenfolge und ihre Auswirkungen zu protokollieren. Diese Protokollierung muss aktiviert werden. Die Anmeldung am MW-System soll mit den Parametern Zeit, Benutzername, entfernte IP-Adresse und eingeräumte Benutzerrechte protokolliert werden. | Mitarbeiter D. exportiert als MW-Nutzer eines Gemeindebüros den Gesamtbestand einer Kirchengemeinde, um die Daten in eine eigene Datenbank zu importieren. Die Datenbank wird anschließend an alle Mitarbeitende der Gemeinde via „Dropbox“ verteilt. Alle Gemeindeglieder erhalten ungefragt wenig später ein Angebot einer örtlichen Bank. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Die Aktivierung der Protokollierung ermöglicht u.a. :<br><br>• eine detaillierte Fehleranalyse<br>• Die Wirksamkeit/ Einhaltung der Benutzerordnung zu überprüfen<br>• Sicherheitsverletzungen zu protokollieren<br>• Fehleranalyse im Schadensfall<br>• Ursachenermittlung/ Täterermittlung<br>• Abschreckung von potenziellen Tätern | Durch eine regelmäßige Auswertung der Protokolldaten sollen Verstöße gegen die Benutzerordnung oder vorsätzliche Angriffe auf das System erkannt werden. Findet eine Auswertung der Protokolldaten nicht oder nur unzureichend statt, können diese nicht für Präventivmaßnahmen genutzt werden. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 6.5. Dezentrales PC-System / Client-Richtlinie (Standard?)

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist notwendig, um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der IT-Systeme auszuschließen. Die zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem. | Ein dienstlich genutzes Macbook wird ohne Virenschutz und Firewall betrieben. Ein Mitarbeiter öffnet eine E-Mail mit einem Schädling / Trojaner als Anlage. Der Trojaner übermittelt die Anmeldedaten des Nutzers an einen Kriminellen ins Ausland. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Durch Vorgaben in einer Client-Richtlinie können die Sicherheitsanforderungen an einen sichereren, dezentralen (verteilten) Clientbetrieb definiert werden und die nutzende Stelle auf Einhaltung verpflichtet werden. | Die Client-Richtlinie muss laufend an die aktuellen Erfordernisse angepasst werden. Da der technische Schutz nicht vernetzter Systeme zu einem großen Teil auf einer geeigneten Zugangskontrolle beruht, ist den Empfehlungen des BSI Grundschutzkataloges zu Installation und Betrieb eines dezentralen Clients unbedingt zu folgen. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### 6.6. Benutzerordnung (mögl. Standard)

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| In der Benutzerordnung werden Regelungen getroffen, die eine sichere und effiziente Nutzung der Applikation ermöglichen. Haupt- und ehrenamtliche Nutzer bekommen nur nach Anerkennung der Benutzerordnung Zugang zum System. | Der Zugriff auf das MW darf geographisch nur innerhalb des Raumes der EKIR und nur auf einem dedizierten dienstlichen Rechner erfolgen. Ein Benutzer ist verpflichtet, seinen Arbeitsplatz beim Verlassen des Raumes zu sperren oder sich vom MW abzumelden. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Die Benutzerordnung soll eine effiziente Arbeit mit der Applikation ermöglichen und mögliche (Sicherheits-)Probleme, die verhaltensbedingte Ursachen haben, vermeiden. Die Benutzerordnung ermöglicht eine Standardisierung. | Ein nachweislicher Verstoß gegen die Nutzerordnung kann geahndet werden. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll |

### 6.7. *Vieraugenprinzip (Auslesen des kompletten Datenbestandes und kommunaler Sperrvermerke)*

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Das Auslesen eines Gesamtbestandes einer Kirchengemeinde soll nur nach der Anwendung des Vieraugenprinzips durchführbar sein. Auswertungen i.V. mit kommunalen Sperrvermerken sollen nur nach der Anwendung des Vieraugenprinzips durchführbar sein. Der Prozess sollte vollständig automatisiert erfolgen. | Eine Mitarbeiterin im Gemeindeamt benötigt zur Erstellung einer persönlichen Einladung zum Gemeindefest den Gesamtbestand. Für den Export muss die Mitarbeiterin die elektronische Freigabe einer weiteren autorisierten Person einholen. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| Ein Export in den genannten Fällen stellt ein hohes Sicherheitsrisiko dar und bürgt existentielle Gefahren. Hier soll durch Anwendung des Vieraugenprinzips eine zusätzliche Sicherheitskontrolle eingefügt werden. | Die Anwendung des Vieraugenprinzips darf den täglichen Arbeitsablauf nicht verändern. Der Datenexport Gesamtbestand und der Umgang mit Sperrvermerken soll die absolute Ausnahme sein. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

### *6.8. bei sicherheitsrelevanten Auffälligkeiten automatisiertes Reporting an die nächste höhere Instanz*

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Aufgrund der heutigen, verteilten Systemkonfiguration mit verteilten, ungesteuerten Zugriffspunkten besteht ein hohes Risiko für Datenverlust und Missbrauch von Zugängen (z.B. i.V. mit sogenannten Trojanern). | Über eine IP-Adresse (östliches Europa) werden große Datenexporte durchgeführt mit einer vorhandenen Nutzerkennung eines Gemeindeamtes . |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Im Rahmen einer automatisierten Auswertung (z.B. Benutzerkennung+IP-Adresse+Land+Funktion(Export)) sollen Auffälligkeiten und mögliche Sicherheitsvorfälle automatisch berichtet werden. | • So könnten der Nutzer und die zuständige kirchliche Stelle bei Sicherheitsvorfällen einen entsprechenden Hinweis erhalten und der Sache nachgehen. |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Soll |

### 6.9. *Auditierungsmöglichkeit (Forensische Auswertungsmöglichkeiten)*

| | Version 0.9 vom 17.06.2013 |
|---|---|
| **Beschreibung** | **Beispiele** |
| Die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit dem MW-System und eine mögliche Feststellung eines Tatbestandes und der Täter muss durch Erfassung, Analyse und Auswertung der digitalen Spuren im Zentralsystem möglich sein.<br><br>Ziel ist die Aufdeckung bzw. der Nachweis und die Analyse der Handlungsmuster. | Durch das Ausnutzen einer Sicherheitslücke einer SQL-Datenbank versucht der Angreifer über die Anwendung, die den Zugriff auf die Datenbank bereitstellt (Internet Explorer), eigene Datenbankbefehle einzuschleusen.<br><br>Sein Ziel ist es, Daten auszuspähen, in seinem Sinne zu verändern, die Kontrolle über den Server zu erhalten oder einfach größtmöglichen Schaden anzurichten.<br><br>Nach Erkennung des Vorfalls sollen forensische Daten dazu beitragen, den Täter zu ermitteln. |
| **Begründung/Nutzen** | **Konsequenz/Risiko** |
| • Täter sollen von der jeweiligen kirchlichen Stelle haftbar gemacht werden können.<br>• Mitarbeitende sollen vor einem Missbrauch ihres Zuganges geschützt werden.<br>• IT-Sicherheit soll gewährleistet werden.<br>• Hoher Schutzbedarf aufgrund der Inhalte<br>• Eine Datenmanipulation oder eine Nichtverfügbarkeit des MW-Verfahrens nach einem Angriff soll aufklärbar sein. | |
| | **vertrauliche/schützenswerte Inhalte** |
| **Verbindlichkeitsgrad** | Muss |

**Anhang**

| Anforderungsbereich | Anforderung | vertraulich/schützenswerte Informationen |
|---|---|---|
| Betrieblich | Dienstleistungsvertrag zur Einhaltung der IT Standards | Muss |
| Funktional | Datenübernahme Einwohnermelderegister | Muss |
| | Datenübernahme Kirchengemeinde | Muss |
| | Bereitstellung von Bescheinigungen | Muss |
| | Bereitstellung von Wahlunterlagen | Muss |
| | Kirchenbuch | Muss |
| | Gemeindegliedverzeichnis | Muss |
| | Abbildung Regionalteil | Muss |
| | Abbildung von Gemeindefusionen und Archivierung der Daten nicht mehr existierender Gemeinden | Muss |
| | Übernahme von Daten aus Fremdsystemen | Muss |
| | Statistische Auswertung sowohl im kirchlichen Auftrag (Gemeindearbeit) als auch für den Regionalteil | Muss |
| | Importschnittstelle für regionale Daten | Muss |
| | Auslesen von CSV Daten | Muss |
| | Pflege von Besuchs- und Verteilerbezirken | Muss |
| | Flexible Personen(-kreis) suche / Recherchemöglichkeiten | Muss |
| | Inner- und zwischenkirchlicher Datenaustausch | Muss |
| | Datentransfer an die Kommune | Soll |
| | Anzeigen von aktiven und inaktiven Datensätzen | Muss |
| | Browsergestützter Client | Muss |
| | Export von Kirchenbüchern via pdf.File | Muss |

| | | |
|---|---|---|
| | Ausweisung von inkonsistenten Datensätzen | Muss |
| | Serienbrieferstellung | Muss |
| | Nichtauswertbarkeit Sperrvermerk | Muss |
| | Datenweitergabe an die Einwohnermelderegister | Muss |
| | Datenexport | Muss |
| Gesetzlich | Berücksichtigung des Kirchenmitgliedschaftsgesetzes (RS 10) § 17 | Muss |
| | Berücksichtigung der Verwaltungsordnung (RS 400) § 27 | Muss |
| | Berücksichtigung der Verordnung über das Gemeindegliederverzeichnis (RS 13) | Muss |
| | Berücksichtigung der Kirchenbuchordnung (RS 410) § 5 | Muss |
| | Berücksichtigung des Kirchengesetzes zur Regelung des Meldewesens (RS 435) §§ 1 und 3 | Muss |
| | Berücksichtigung der kommunalen Meldegesetze | Muss |
| | Grundgesetz (Art. 4) | Muss |
| | Datenschutzverordnung unter Berücksichtigung der staatlichen Regelungen | Muss |
| | geklärte Verfahrensverantwortung | Muss |
| Non-funktional | Herstellersupport | Muss |
| | intuitive Benutzeroberfläche | Muss |
| Sicherheit | Prozesses des IT-Sicherheitsmanagements | Muss |
| | Sicherer Verfahrensbetrieb undgesicherte Betriebsumgebung | Muss |
| | Datensicherung im Rechenzentrum | Muss |
| | Benutzeraktivitätsprotokoll | Muss |
| | Dezentrales PC-System / | Muss |

| | | |
|---|---|---|
| | Client-Richtlinie | |
| | Benutzerordnung | Muss |
| | Vieraugenprinzip | Muss |
| | Bei sicherheitsrelevanten Auffälligkeiten automatisiertes Reporting an die nächste höhere Instanz | Soll |
| | Auditierungsmöglichkeit | Muss |

R = (Durchführungsverantwortung / Responsible)
A = (Gesamtverantwortung / Accountable)
C = (Beratende Funktion / Consulted)
I = (Informationsbeziehung/Informed)

| Prozess | strukturierte Aufgabenliste | Aufgabe wird heute min. punktuell erbracht | Pflichtaufgabe (selber durchzuführen) | potentielles Outsourcing | Mitarbeitende IT-Koordination | Leitung IT-Koordinoation (Regionen) | IT-Betreuung | Zentrale Kompetenzzentren |
|---|---|---|---|---|---|---|---|---|
| System | Lokale Netzwerke planen (LAN in Gemeinden, Kirchenkreise, Verwaltung) | X | | x | R | R | A | C |
| | IT-Koordination bei Aufbau und Planung von Standort-LAN beraten | | x | | C | C | C | A/R |
| | Systemkomponenten für lokale Kommunikation/ Netze / TK planen | X | | x | R | R | A | C |
| System Implementation & Dep | Betriebsverfahren für LAN-Systeme entwickeln | X | x | | R | R | A | C |
| | LAN-Systeme aufbauen | X | | x | R | R | A | C |
| | LAN-Systeme anbinden | X | | x | R | R | A | C |
| | LAN-Systeme testen | X | x | | R | R | A | C |
| | LAN-Systeme in Betrieb nehmen | X | x | | R | R | A | C |
| | Betriebsverfahren für Systemkomponenten für die lokale Kommunikation/Netze/TK entwickeln | X | x | | R | R | A | C |
| | Systemkomponenten für die lokale Kommunikation/Netze/TK aufbauen | X | | x | R | R | A | C |
| | Systemkomponenten für die lokale Kommunikation/Netze/TK anbinden | X | | x | R | R | A | C |
| | Systemkomponenten für die lokale Kommunikation/Netze/TK testen | X | x | | R | R | A | C |
| | Systemkomponenten für die lokale Kommunikation/Netze/TK in Betrieb nehmen | X | x | | R | R | A | C |
| System Operations | Systembetrieb für den Bereich IT-Service Ausstattung steuern | X | x | | C | C | | A/R |
| | Hardwarekonfiguration für die IT-Ausstattung Standort ändern | X | | x | R | A/R | I | C |
| | Hardwarekonfiguration für die lokale Kommunikation/ Netze/ TK ändern | X | | x | R | A/R | I | C |
| | Clients/dezentrale Hardware für die IT-Ausstattung Arbeitsplatz ändern | X | | x | R | R | A | C |
| | Nutzerprofile für die IT-Ausstattung Arbeitsplatz einrichten und ändern | X | x | | R | R | A | C |
| | Zugriffsrechte für die IT-Ausstattung Arbeitsplatz einrichten und ändern | X | x | | R | R | A | C |
| | Virenschutz für die IT -Arbeitsplatzsysteme aktualisieren | X | | x | R | R | A | C |
| | Konfigurationsänderungen für lokale IT-Ausstattung dokumentieren | x | | x | R | R | A | C |
| | Konfigurationsänderungen für IT-Basisdienste dokumentieren | X | | x | | | C | A/R |
| | Arbeitsplatz-IT nach Vorgabe der IT-Ausstattung steuern (Clients) | X | x | | R | R | A | C |
| | Standort-IT nach Vorgabe der IT-Ausstattung steuern (MFD, Telefonanlage) | X | x | | R | R | A | C |
| | IT-Verbrauchsmaterial steuern | X | x | | R | R | A | |
| | Lokale IT-Betriebsräume steuern | X | x | | R | R | A | C |
| Consulting | Applikationsbedarf der Kunden identifizieren und bewerten | X | x | | R | R | A | C |
| | Applikationsbedarf für die Fachanwendung Meldewesen identifizieren und bewerten | X | | | | C | I | A/R |
| | Applikationsbedarf für die Fachanwendungen Finanzwesen/Fundraising identifizieren und bewerten | X | | | | C | I | A/R |
| | Applikationsbedarf für die Fachanwendungen HR/Verwaltung identifizieren und bewerten | X | | | | C | I | A/R |
| | Applikationsbedarf für die Fachanwendungen Liegenschaftsmanagement identifizieren und bewerten | X | | | | C | I | A/R |
| | Applikationsbedarf für die Fachanwendungen Theologie/Bildung/Erziehung identifizieren und bewerten | X | | | | C | I | A/R |
| | Anforderungen für die IT-Ausstattung der Standorte qualifizieren | X | x | | R | R | A | C |
| | Anforderungen für die IT-Ausstattung der Arbeitsplätze qualifizieren | X | x | | R | R | A | C |
| | Anforderungen für die Fachanwendung Meldewesen qualifizieren | X | | | | C | I | A/R |
| | Anforderungen für die Fachanwendungen Finanzwesen/Fundraising qualifizieren | X | | | | C | I | A/R |
| | Anforderungen für die Fachanwendungen HR/Verwaltung qualifizieren | X | | | | C | I | A/R |
| | Anforderungen für die Fachanwendungen Liegenschaftsmanagement qualifizieren | X | | | | C | I | A/R |
| | Anforderungen für die Fachanwendungen Theologie/Bildung/Erziehung qualifizieren | X | | | | C | I | A/R |

R = (Durchführungsverantwortung / Responsible)
A = (Gesamtverantwortung / Accountable)
C = (Beratende Funktion / Consulted)
I = (Informationsbeziehung/Informed)

| Prozess | strukturierte Aufgabenliste | Aufgabe wird heute min. punktuell erbracht | Pflichtaufgabe (selber durchzuführen) | potentielles Outsourcing | Mitarbeitende IT-Koordination | Leitung IT-Koordinoation (Regionen) | IT-Betreuung | Zentrale Kompetenzzentren |
|---|---|---|---|---|---|---|---|---|
| Application | Applikationseinsatz und-nutzung für die IT-Arbeitplätze optimieren | X | | | | C | | A/R |
| | Applikationseinsatz und-nutzung für die Fachanwendung Meldewesen optimieren | X | | | | C | I | A/R |
| | Applikationseinsatz und-nutzung für die Fachanwendungen Finanzwesen/Fundraising optimieren | X | | | | C | | A/R |
| | Applikationseinsatz und-nutzung für die Fachanwendungen HR/Verwaltung optimieren | X | | | | C | | A/R |
| | Applikationseinsatz und-nutzung für die Fachanwendungen Liegenschaftsmanagement optimieren | X | | | | C | | A/R |
| | Applikationseinsatz und-nutzung für die Fachanwendungen Theologie/Bildung/Erziehung optimieren | X | | | | C | | A/R |
| | Anforderungsänderungen für die IT-Ausstattung Arbeitsplatz steuern | X | | | | C | | A/R |
| | Anforderungsänderungen für die IT-Ausstattung Standort steuern | X | | | | C | | A/R |
| | Anforderungsänderungen für die Fachanwendung Meldewesen steuern | X | | | | C | | A/R |
| | Anforderungsänderungen für die Fachanwendungen Finanzwesen/Fundraising steuern | X | | | | C | | A/R |
| | Anforderungsänderungen für die Fachanwendungen HR/Verwaltung steuern | X | | | | C | | A/R |
| | Anforderungsänderungen für die Fachanwendungen Liegenschaftsmanagement steuern | X | | | | C | | A/R |
| | Anforderungsänderungen für die Fachanwendungen Theologie/Bildung/Erziehung steuern | X | | | | C | | A/R |
| Application & Releas | Anwendungssoftware die IT-Ausstattung Arbeitsplatz evaluieren und auswählen | | | | | C | I | A/R |
| | Releases für die Arbeitsplatzsoftware definieren und planen | | | | | C | | A/R |
| | Releases für die Fachanwendung Meldewesen definieren und planen | | | | | C | | A/R |
| | Releases für die Fachanwendungen Finanzwesen/Fundraising definieren und planen | | | | | C | | A/R |
| | Releases für die Fachanwendungen HR/Verwaltung definieren und planen | | | | | C | | A/R |
| | Releases für die Fachanwendungen Liegenschaftsmanagement definieren und planen | | | | | C | | A/R |
| | Releases für die Fachanwendungen Theologie/Bildung/Erziehung definieren und planen | | | | | C | | A/R |
| App | Betriebsverfahren für die Arbeitsplatz-IT steuern und entwickeln | X | x | | R | R | I | A |
| Application Operation & Support | Anwendungskonfiguration für die IT-Ausstattung Arbeitsplatz ändern | X | x | | R | R | A | C |
| | Anwenderprofile für die IT Arbeitsplätze ändern | X | x | | R | R | A | C |
| | Zugriffrechte für die Fachanwendung Meldewesen einrichten und ändern | X | x | | R | R | A | C |
| | Zugriffrechte für die Fachanwendungen Finanzwesen/Fundraising einrichten und ändern | X | x | | R | R | A | C |
| | Zugriffsrechte für die Fachanwendungen HR/Verwaltung einrichten und ändern | X | x | | R | R | A | C |
| | Zugriffsrechte für die Fachanwendungen Liegenschaftsmanagement/Friedhofsverwaltung einrichten und ändern | X | x | | R | R | A | C |
| | Zugriffsrechte für die Fachanwendung Theologie/Bildung/Erziehung einrichten und ändern | X | x | | R | R | A | C |
| | Konfigurationsänderungen für die IT-Ausstattung Arbeitplatz dokumentieren | X | | x | R | R | A | |
| | Konfigurationsänderungen für die IT-Service Ausstattung dokumentieren | X | | x | R | R | A | |
| | Konfigurationsänderungen für die lokale Kommunikation/Netze/TK dokumentieren | X | | x | R | R | A | |
| | Anwenderbetreuung im 1st Level Support durchführen | X | | x | R | A/R | | |
| | Anwenderbetreuung im 1st Level Support steuern | | | | | C | A/R | |
| | Schulungsbedarf für IT-Arbeitsplatz ermitteln | X | x | | R | R | A | C |
| | Schulungsbedarf für die Fachanwendungen ermitteln | X | x | | R | R | A | C |
| | Schulungskonzept erstellen | X | | x | R | R | A | C |
| | Schulungsunterlagen erstellen und pflegen | X | | x | R | R | A | C |
| | Anwenderschulungen planen und organisieren | X | | x | R | R | A | C |

R = (Durchführungsverantwortung / Responsible)
A = (Gesamtverantwortung / Accountable)
C = (Beratende Funktion / Consulted)
I = (Informationsbeziehung/Informed)

| Prozess | strukturierte Aufgabenliste | Aufgabe wird heute min. punktuell erbracht | Pflichtaufgabe (selber durchzuführen) | potentielles Outsourcing | Mitarbeitende IT-Koordination | Leitung IT-Koordinoation (Regionen) | IT-Betreuung | Zentrale Kompetenzzentren |
|---|---|---|---|---|---|---|---|---|
| | Anwenderschulungen durchführen | X | x | R | A/R | I | C | |
| | Schulungsteilnahme protokollieren | X | x | R | R | A | | |
| Business Relationship M | Kundenbeziehung steuern | X | x | R | R | A | | |
| | Kundenbedarfe steuern | X | x | R | R | A | | |
| | Beschwerden managen | X | x | R | R | A | | |
| | Konflikte deeskalieren | X | x | R | R | A | | |
| | Best Practice Transfer sicherstellen | X | x | R | R | A | C | |
| | Innovationsberatung für Kunden durchführen | X | x | R | R | A | C | |
| | Kundenerwartungen verstehen | X | x | R | R | A | | |
| | Geschäftsprozess- und Methodenberatung | X | x | R | R | A | C | |
| Supplier Management | Lieferantenbeziehungen und -verträge für die IT-Ausstattung Standort identifizieren und evaluieren | X | x | R | R | A | | |
| | Lieferantenbeziehungen und -verträge für die IT-Ausstattung Arbeitsplatz identifizieren und evaluieren | X | x | R | R | A | | |
| | Lieferantenbeziehungen und -verträge die lokale Kommunikation/Netze/TK identifizieren und evaluieren | X | x | R | R | A | | |
| | Supplier für die IT-Ausstattung Standort auswählen | X | x | R | R | A | C | |
| | Supplier für die IT-Ausstattung Arbeitsplatz auswählen | X | x | R | R | A | C | |
| | Supplier die lokale Kommunikation/Netze/TK auswählen | X | x | R | R | A | C | |
| | Supplierbeziehungen für die IT-Ausstattung Standort steuern | X | x | R | R | A | | |
| | Supplierbeziehungen für die IT-Ausstattung Arbeitsplatz steuern | X | x | R | R | A | | |
| | Supplierbeziehungen die lokale Kommunikation/Netze/TK steuern | X | x | R | R | A | | |
| | Supplieranforderungen für die IT-Ausstattung Standort managen | X | x | R | R | A | | |
| | Supplieranforderungen für die IT-Ausstattung Arbeitsplatz managen | X | x | R | R | A | | |
| | Supplieranforderungen die lokale Kommunikation/Netze/TK managen | X | x | R | R | A | | |
| | Supplierkonflike für die IT-Ausstattung Standort eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike für die IT-Ausstattung Arbeitsplatz eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike für die Fachanwendung Meldewesen eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike für die Fachanwendungen Finanzwesen/Fundraising eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike für die Fachanwendungen HR/Verwaltung eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike für die Fachanwendungen Liegenschaftsmanagement/ Friedhofsverwaltung eskalieren und deses | X | x | R | R | A | C | |
| | Supplierkonflike für die Fachanwendungen Theologie/ Bildung/ Erziehung eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike das Daten- und Speicher Management eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike die lokale Kommunikation/Netze/TK eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike die zentrale Kommunikation/Netze/TK eskalieren und deseskalieren | X | x | R | R | A | C | |
| | Supplierkonflike die Server- und Betriebsumgebungen eskalieren und deseskalieren | X | x | R | R | A | C | |
| alog Manageme | IT-Services Ausstattung spezifizieren | | | | C | I | A/R | |
| | IT-Services Fachanwendungen spezifizieren | | | | C | I | A/R | |
| | IT-Services für IT-Basisdienste spezifizieren | | | | C | I | A/R | |
| | Servicekatalog für die IT-Services Ausstattung pflegen | | | | C | I | A/R | |
| | Servicekatalog für die IT-Services Fachanwendungen pflegen | | | | C | I | A/R | |

R = (Durchführungsverantwortung / Responsible)
A = (Gesamtverantwortung / Accountable)
C = (Beratende Funktion / Consulted)
I = (Informationsbeziehung/Informed)

| Prozess | strukturierte Aufgabenliste | Aufgabe wird heute min. punktuell erbracht | Pflichtaufgabe (selber durchzuführen) | potentielles Outsourcing | Mitarbeitende IT-Koordination | Leitung IT-Koordinoation (Regionen) | IT-Betreuung | Zentrale Kompetenzzentren |
|---|---|---|---|---|---|---|---|---|
| Service Catal | Servicekatalog für die IT-Basisdienste pflegen | | | | C | I | A/R | |
| | Servicekatlalog für die IT-Services Ausstattung kommunizieren | | x | R | R | A | C | |
| | Servicekatlalog für die IT-Services Fachanwendungen kommunizieren | | x | R | R | A | C | |
| | Servicekatlalog für die IT-Basisdienste kommunizieren | | x | R | R | A | C | |
| Availibility & Capacity Management | Verfügbarkeitsbedarf für die IT-Services Ausstattung ermitteln und bewerten | X | | | C | I | A/R | |
| | Verfügbarkeitsbedarf für die IT-Services Fachanwendungen ermitteln und bewerten | X | | | C | I | A/R | |
| | Verfügbarkeitsbedarf für die IT-Basisdienste ermitteln und bewerten | X | | | C | I | A/R | |
| | Leistungsbedarf, Verfügbarkeit und Kapazität für die IT-Services Ausstattung ermitteln und bewerten und Referen | X | | | C | I | A/R | |
| | Leistungsbedarf, Verfügbarkeit und Kapazität für die IT-Services Fachanwendungen ermitteln und bewerten und R | X | | | C | I | A/R | |
| | Leistungsbedarf, Verfügbarkeit und Kapazität für die IT-Basisdienste ermitteln und bewerten und Referenz erstelle | X | | | C | I | A/R | |
| | Geschäftliche Auswirkungen für die IT-Services Ausstattung beurteilen | X | | | C | I | A/R | |
| | Geschäftliche Auswirkungen für die IT-Services Fachanwendungen beurteilen | X | | | C | I | A/R | |
| | Geschäftliche Auswirkungen für die IT-Basisdienste beurteilen | X | | | C | I | A/R | |
| | Verfügbarkeits-, Leistungs- und Kapazitätsschwierigkeiten für die IT-Services Ausstattung untersuchen und behebe | X | | | C | I | A/R | |
| | Verfügbarkeits-, Leistungs- und Kapazitätsschwierigkeiten für die IT-Services Fachanwendungen untersuchen und | X | | | C | I | A/R | |
| | Verfügbarkeits-, Leistungs- und Kapazitätsschwierigkeiten für die IT-Basisdienste untersuchen und beheben | X | | | C | I | A/R | |
| Request Fulfill | Aufträge annehmen, klassifizieren und priorisieren | X | x | R | R | A | | |
| | Auftragsgenehmigung einholen | X | x | R | R | A | | |
| | Auftragsausführung verifizieren, genehmigen und ausführen | X | x | R | R | A | | |
| | Auftragsausführung steuern, verfolgen und berichten | X | x | R | R | A | | |
| | Aufträge abschließen | X | x | R | R | A | | |
| Event Management | Lokale IT-Systeme überwachen | X | x | R | R | A | | |
| | Zentrale IT-Systeme überwachen | X | | | C | I | A/R | |
| | Lokale Anwendungsverfügbarkeit überwachen | X | x | R | R | A | | |
| | Zentrale Anwendungsverfügbarkeit überwachen | X | | | C | I | A/R | |
| | Lokale Infrastrukturverfügbarkeit überwachen | X | x | R | R | A | | |
| | Zentrale Infrastrukturverfügbarkeit überwachen | X | | | C | I | A/R | |
| | Events (Systemmeldungen) qualifizieren und bewerten | X | | | C | I | A/R | |
| Incident Managen | Störungen annehmen und priorisieren | X | x | R | A/R | I | | |
| | Störungen untersuchen, diagnostizieren und sammeln | X | x | R | A/R | I | C | |
| | Störungen beheben | X | x | R | A/R | I | C | |
| | Störungsbehebung eskalieren | X | x | R | A/R | I | | |
| | Störungsbehebung steuern, verfolgen und berichten | X | x | R | A/R | I | | |
| | Störungen abschließen | X | x | R | A/R | I | | |
| 1st Level | Service Requests annehmen und klassifizieren | X | x | R | A/R | I | | |
| | Anwenderfragen beantworten | X | x | R | A/R | I | | |
| | Anwender aktiv informieren | X | x | R | A/R | I | | |
| | Probleme identifizieren und klassifizieren | X | | | C | C | A/R | |

R = (Durchführungsverantwortung / Responsible)
A = (Gesamtverantwortung / Accountable)
C = (Beratende Funktion / Consulted)
I = (Informationsbeziehung/Informed)

| Prozess | strukturierte Aufgabenliste | Aufgabe wird heute min. punktuell erbracht | Pflichtaufgabe (selber durchzuführen) | potentielles Outsourcing | Mitarbeitende IT-Koordination | Leitung IT-Koordinoation (Regionen) | IT-Betreuung | Zentrale Kompetenzzentren |
|---|---|---|---|---|---|---|---|---|
| Problem Management | Probleme diagnostizieren | X | | | | C | C | A/R |
| | Problemlösung steuern & verfolgen | X | | | | C | C | A/R |
| | Problemlösung entwerfen und testen | X | | | | C | C | A/R |
| | Work arounds bereitstellen | X | | | | C | C | A/R |
| | Problemlösung für Major Problems überprüfen | X | | | | C | C | A/R |
| | Lösungswissen sichern & bereitstellen | X | | | | C | C | A/R |
| | Fehlerbehebung verfolgen | X | | | | C | C | A/R |
| | Fehler beheben | X | | | | C | C | A/R |
| | Probleme abschließen | X | | | | C | C | A/R |
| | Störungsaufkommen & Trends analysieren | | | | | C | C | A/R |
| Access M | Zugriffsanforderungen bewerten | | x | | R | A/R | I | |
| | Nutzer- und Zugriffsprofile zyklisch überprüfen | | | x | R | A/R | I | |
| | Zugriffsprotokolle auswerten und kontrollieren | | | x | R | A/R | I | |
| Change Management | Änderungen beantragen | X | | | | R | I | A/R |
| | Änderungen an Standort-Infrastruktur genehmigen | X | x | | R | A/R | I | |
| | Änderungen an zentralen Standaort-Infrastrukturkomponenten genehmigen | x | | | | C | | A/R |
| | Änderungen an IT-Arbeitsplatz (Einzel) genehmigen | x | x | | R | A/R | I | |
| | Änderungen an zentralen IT-Arbeitsplatz-Komponeten genehmigen | X | | | | C | I | A/R |
| | Änderungen für die Fachanwendung Meldewesen planen | X | | | | C | I | A/R |
| | Änderungen für die Fachanwendungen Finanzwesen/Fundraising planen | X | | | | C | I | A/R |
| | Änderungen für die Fachanwendungen HR/Verwaltung planen | X | | | | C | I | A/R |
| | Änderungen für die Fachanwendungen Liegenschaftsmanagement/Friedhofsverwaltung planen | X | | | | C | I | A/R |
| | Änderungen für die Fachanwendungen Theologie/Bildung/Erziehung planen | X | | | | C | I | A/R |
| | Änderungen für das Daten- und Speichermanagement planen | X | | | | C | I | A/R |
| | Änderungen für Kommunikation/Netze/TK planen | X | | | | C | I | A/R |
| | Änderungen für die Server- und Betriebsumgebung planen | X | | | | C | I | A/R |
| | Änderungen testen | X | | x | R | A/R | I | |
| | Änderungen an Standort-Infrastruktur planen | X | | x | R | A/R | I | |
| | Änderungen an zentralen Standaort-Infrastrukturkomponenten planen | x | | | | C | | A/R |
| | Änderungen an IT-Arbeitsplatz (Einzel) planen | x | | x | R | A/R | I | |
| | Änderungen an zentralen IT-Arbeitsplatz-Komponeten planen | X | | | | C | I | A/R |
| | Änderungen kommunizieren | X | | x | R | A/R | I | |
| | Änderungen abnehmen | X | x | | R | A/R | I | |
| | Änderungsaufgaben koordinieren, verfolgen und berichten | X | | x | R | A/R | I | |
| | Änderungen abschließen | X | | x | R | A/R | I | |
| gement | IT-Anlagegüter identifizieren und katalogisieren | X | x | | R | R | A | |
| | Verträge managen | X | x | | R | R | A | |
| | Wartung planen und steuern | X | x | | R | R | A | |

R = (Durchführungsverantwortung / Responsible)
A = (Gesamtverantwortung / Accountable)
C = (Beratende Funktion / Consulted)
I = (Informationsbeziehung/Informed)

| Prozess | strukturierte Aufgabenliste | Aufgabe wird heute min. punktuell erbracht | Pflichtaufgabe (selber durchzuführen) | potentielles Outsourcing | Mitarbeitende IT-Koordination | Leitung IT-Koordinoation (Regionen) | IT-Betreuung | Zentrale Kompetenzzentren | |
|---|---|---|---|---|---|---|---|---|---|
| Asset Manag | Betreute Hardware managen | X | x | R | R | A | | | |
| | Software und Lizenzen managen | X | x | R | R | A | | | |
| | Lebenszyklus für Anlagegüter steuern | X | x | R | R | A | | | |
| | IT-Anlagegüter verwalten | X | x | R | R | A | | | |
| | Anlagevermögen und -kosten optimieren | X | x | R | R | A | | | |
| Configuration Ma | Konfigurationselemente für IT-Ausstattung Standort pflegen und steuern | | x | R | R | A | | | |
| | Konfigurationselemente für IT-Ausstattung Arbeitsplatz pflegen und steuern | | x | R | R | A | | | |
| | Konfigurationselemente für lokale Kommunikation/Netze/TK pflegen und steuern | | x | R | R | A | | | |
| | Konfigurationsstatus für IT-Ausstattung Standort verfolgen und berichten | | x | R | R | A | | | |
| | Konfigurationsstatus für IT-Ausstattung Arbeitsplatz verfolgen und berichten | | x | R | R | A | | | |
| | Konfigurationsstatus für lokale Kommunikation/Netze/TK verfolgen und berichten | | x | R | R | A | | | |
| IT Org | IT-Prozessentwicklung managen | | | | | C | | | A/R liegt in der Stabsfunktion Prozesskoordination/Revision/QM |
| | IT-Prozesssteuerung managen | | | | | C | | | dito |
| IT-Inn | Technologische Entwicklung überwachen und beobachten | X | | | C | I | A/R | | |
| | Potenzial aufkommender Technologien und innovativer Ideen beurteilen | | | | C | I | A/R | | |
| IT-Personalmanag | adäquate und angemessene Personalbesetzung aufrechterhalten | X | x | R | R | I | R | | A liegt in der Querschnittsfunktion Strategie/Organisation/Personal |
| | Leistungsträger der IT identifizieren | | x | R | R | I | R | | dito |
| | Fähigkeiten und Kompetenzen der Mitarbeiter aufrechterhalten | | x | R | R | I | R | | dito |
| | Mitarbeiterleistung bewerten | | x | R | R | I | R | | dito |
| | Einsatze von IT- und Fachbereichspersonal planen und verfolgen | | x | R | R | I | R | | dito |
| | Vertragspersonal managen | X | x | R | R | I | R | | dito |
| alitätsmana | Qualitätsmanagement-System einrichten | X | | | | C | C | | A/R liegt in der Stabsfunktion Prozesskoordination/Revision/QM |
| | Qualitätsstandards, -praktiken und –verfahren definieren und managen | X | x | | C | R | R | | dito |
| | Qualitätsmanagement am Kunden ausrichten | X | x | | C | R | R | | dito |
| | Qualitätsüberwachung, Kontrollen und Überprüfungen durchführen | X | x | | C | R | R | | dito |

R = (Durchführungsverantwortung / Responsible)
A = (Gesamtverantwortung / Accountable)
C = (Beratende Funktion / Consulted)
I = (Informationsbeziehung/Informed)

| Prozess | strukturierte Aufgabenliste | Aufgabe wird heute min. punktuell erbracht | Pflichtaufgabe (selber durchzuführen) | potentielles Outsourcing | Mitarbeitende IT-Koordination | Leitung IT-Koordinoation (Regionen) | IT-Betreuung | Zentrale Kompetenzzentren | |
|---|---|---|---|---|---|---|---|---|---|
| IT-Qu | Qualitätsmanagement in Lösungen, die Entwicklung integrieren und Servicebereitstellung unterstützen | X | x | | C | R | R | | dito |
| | Kontinuierliche Verbesserung sicherstellen | X | x | | C | R | R | | dito |
| IT-Risikomanagement | Risikomanagement evaluieren | | | | | C | | | A/R liegt in der Stabsfunktion Prozesskoordination/Revision/QM |
| | Risikomanagement steuern | | x | | C | R | R | | dito |
| | Risiken erfassen | | x | | C | R | R | | dito |
| | Risiko analysieren | | x | | C | R | R | | dito |
| | Risikoprofil pflegen | | x | | C | R | R | | dito |
| | Risiko artikulieren | | x | | C | R | R | | dito |
| | Portfolio für Risikomanagement-Maßnahmen definieren | | x | | C | R | R | | dito |
| | Risiko behandeln | | x | | C | R | R | | dito |
| IT-Programm- und Proje | IT-Projekte starten und initiieren | | | | C | C | A/R | | |
| | IT-Projekte planen | | | | C | C | A/R | | |
| | IT-Projektqualität managen | | | | C | C | A/R | | |
| | IT-Projektrisiken managen | | | | C | C | A/R | | |
| | IT-Projekte überwachen und steuern | | | | C | C | A/R | | |
| | IT-Projektressourcen und Arbeitspakete managen | | | | C | C | A/R | | |
| | IT-Projekte abschließen | | | | C | C | A/R | | |
| | IT-Projekte evaluieren | | | | C | C | A/R | | |
| IT-Knowledge | Wissentransfer pflegen und fördern | | x | A/R | A/R | A/R | A/R | | |
| | Informationsquellen identifizieren und klassifizieren | | x | A/R | A/R | A/R | A/R | | |
| | Informationen verarbeiten und daraus nutzbares Wissen ableiten | | x | A/R | A/R | A/R | A/R | | |
| | Wissen nutzen und in praktikablerForm weitergeben | X | x | A/R | A/R | A/R | A/R | | |
| | regelmäßig die Aktualität von Informationen und Wissen bewerten | | x | A/R | A/R | A/R | A/R | | |
| Leistung | Leistungs- und Konformitätsdaten für die IT-Ausstattung Standort erfassen und verarbeiten | | x | R | R | I | A | | |
| | Leistungs- und Konformitätsdaten für die IT-Ausstattung Arbeitsplatz erfassen und verarbeiten | | x | R | R | I | A | | |
| | Leistungs- und Konformitätsdaten für Kommunikation/Netze/TK erfassen und verarbeiten | | | | C | I | A/R | | |
| Internes Kontrollsystem | Interne Kontrollen überwachen | | | | | C | | | A/R liegt im IT-Beirat |
| | Effektivität von Geschäftsprozesskontrollen überprüfen | | | | | C | | | dito |
| | Selbsteinschätzung zu Kontrollen durchführen | | | | | C | | | dito |
| | Kontrollschwächen identifizieren und melden | | | | | C | | | dito |
| | Unabhängigkeit und Qualität der Prüfer sicherstellen | | | | | C | | | dito |
| | Prüfinitiativen planen | | | | | C | | | dito |
| | Umfang von Prüfinitiativen festlegen | | | | | C | | | dito |
| | Prüfinitiativen umsetzen | | | | | C | | | dito |
| Compliance | Externe Compliance-Anforderungen identifizieren | X | x | R | R | R | R | | A liegt in der Stabsfunktion Prozesskoordination/Revision/QM |
| | Reaktion auf externe Compliance-Anforderungen optimieren | | x | R | R | R | R | | dito |
| | Externe Compliance bestätigen | | x | R | R | R | R | | dito |
| | Compliance-Bestätigungen erhalten | | x | R | R | R | R | | dito |