Evangelische Landeskirche
In Württemberg

IT-Konzept

der
Evangelischen Landeskirche
in Württemberg

Stuttgart, im November 2012

Herausgegeben von

Referat Informationstechnologie
Evangelischer Oberkirchenrat
Gänsheidestraße 4
70184 Stuttgart

I Vorwort zum IT-Konzept 2007

1. Rückblick

Mit dem IT-Konzept der Evangelischen Landeskirche in Württemberg wurde im Jahr 2005 erstmalig in einer Zusammenstellung der technische, organisatorische und rechtliche Rahmen für den Einsatz von Informationstechnologie im Bereich der Evangelischen Landeskirche in Württemberg beschrieben.

Dafür gab es interne und externe Anstöße, die auch heute noch gelten, zum Teil haben sich die Dinge in der Richtung entwickelt, wie wir im Jahr 2005 vermutet haben.

Mit der vorliegenden aktuellen Fassung haben wir der Entwicklung im IT-Bereich in den letzten beiden Jahren Rechnung getragen und präsentieren Ihnen den aktuellen Rahmen für den Einsatz von IT in der Landeskirche Württemberg.

Folgende Trends haben sich weiterentwickelt und werden auch für die Zukunft in der IT Maßstäbe setzen:

- Bisher aufwendig gepflegte lokale Lösungen werden zunehmend durch zentral angebotene Komplettlösungen ersetzt, nicht zuletzt aus Kostengründen.
- In Verbindung mit der Anwendung definierter Standards kann eine Vereinfachung erreicht werden.
- Das Thema Datensicherheit und Datenschutz stellt bezüglich der Umsetzung immer höhere Anforderungen an die IT.

Unter Beachtung dieser Rahmenbedingungen haben wir begonnen, das Serviceangebot des Referats IT für Kirchenbezirke und -gemeinden auszuweiten. Bereits jetzt werden größere Verwaltungseinheiten im Bereich der Kirchlichen Verwaltungsstellen und Kirchenpflegen zusammen mit den Arbeitsplätzen des OKR in einem Netz betreut.

Für weitere kirchliche Verwaltungen in Kirchenpflegen und Verwaltungsstellen werden wir die Integration in das Netz anbieten.

Dabei gehen wir davon aus, dass insgesamt eine Kostensenkung im IT-Bereich erreicht werden kann, wenn die vorgenannten Ziele systematisch verfolgt werden. An den gesunkenen Verrechnungspreisen in Anlage 3 sind diese Veränderungen bereits abzulesen. Gleichzeitig ergeben sich für die kirchlichen Verwaltungen qualitative Verbesserungen im täglichen Betriebsablauf, der ohne eine funktionierende EDV heutzutage nicht mehr denkbar ist. Hier spielt auch das Thema Datensicherheit eine zunehmend wichtigere Rolle. im Bereich der Informationstechnologie im OKR werden die Vorgaben zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnologie schrittweise umgesetzt, die Zertifizierung in der ersten Stufe ist für 2007 vorgesehen.

2. Perspektiven

- *weitergehende Unterstützung*

  Die Reaktionen auf das IT-Konzept und die Rückmeldungen, die wir in der EDV-Kommission erhalten, zeigen deutlich, dass auf allen Verwaltungsebenen innerhalb der Landeskirche der Wunsch nach einer weitergehenden Unterstützung im EDV-Bereich besteht. Unter dem Stichwort "EDV im Pfarramt" hat sich in der EDV-Kommission bereits eine Grundsatzdebatte entwickelt. Es ist aufgrund der

vorhandenen komplexen Strukturen hier nicht mit schnellen Ergebnissen für die Betroffenen zu rechnen, aber das Thema wird in der nächsten Zeit angegangen und weiter verfolgt werden.

- *elektronische Kommunikation/eGovernment*

  Der elektronische Datenaustausch zwischen den Dienststellen hat weiter zugenommen. Um diesen sicherer zu machen, wurde in einem ersten Schritt jetzt die DatenverschlüsselungsVO technisch umgesetzt. Damit ist es möglich, E-Mails, die personenbezogene Daten beinhalten, verschlüsselt zu versenden.

  Die lange angekündigte und bereits gesetzlich verankerte "digitale Signatur" lässt hingegen weiterhin in der Umsetzung auf praxistaugliche Verfahren auf sich warten. Es ist aber davon auszugehen, dass der Umgang mit der digitalen Signatur künftig zum Standard in der elektronischen Kommunikation werden wird.

- *Schriftgutverwaltung/elektronische Vorgangsbearbeitung*

  Im Oberkirchenrat wurde jetzt mit dem Projekt "ePersAkte" im Bereich der Personalverwaltung für Pfarrerinnen und Pfarrer der Einstieg in die elektronische Vorgangsbearbeitung gewagt. Schon in der Anfangsphase zeigt sich, dass die Umsetzung entscheidend von den organisatorischen Vorarbeiten (beginnend mit einer umfassenden Beschreibung der Geschäftsprozesse) abhängig ist. Konkret ist für eine elektronische Vorgangsbearbeitung zu allererst ein funktionierender aktueller Aktenplan notwendig.

- *Portale/mobiler Zugriff*

  An verschiedenen Stellen haben wir mittlerweile die Möglichkeit, über Portale auf Informationen in der Landeskirche zugreifen zu können. Von der Abdeckung des einfachen Informationsbedarfs, wie er über den Internetauftritt der Landeskirche und das Bildungsportal möglich ist, bis zum Zugriff auf konkrete Anwendungen reicht die Spanne.

  Im Bereich des neuen Kirchlichen Finanzmanagements bieten wir mit unserem CITRIX-Portal hier einen komfortablen und zugleich sicheren Zugriff auf die jeweils eigenen Daten der Dienststelle.

  Der weitere Ausbau dieses Angebots ist absehbar. Mit dieser Technik wird auch die Telearbeit weiter gefördert, da außer einem funktionierenden Internetzugang keine zusätzlichen Anforderungen vor Ort benötigt werden, die Daten liegen geschützt und gesichert hinter der Firewall der zentralen Serverumgebung.

- *Fundraising*

  Unter dieser englischen Vokabel wird gemeinhin das professionelle Einwerben von Spenden verstanden. Dafür stehen verschiedene (Standard)-Anwendungen im EDV-Bereich zur Verfügung. Wir prüfen derzeit mit dem Fundraising-Beauftragten der Landeskirche und betroffenen Dienststellen in der Landeskirche und im OKR deren Praxistauglichkeit. Es ist davon auszugehen, dass am Ende dieser Prüfung die Aufnahme einer Software in die Liste der Grundverfahren stehen wird.

3. Ziele und Rahmenbedingungen (aus dem IT-Konzept 2005)

Die Informationstechnologie der Evangelischen Landeskirche Württemberg, nachstehend IT genannt, unterstützt die Verwaltung im Oberkirchenrat und in den Dienststellen in den Kirchengemeinden und -bezirken der Landeskirche. Sie stellt im Rahmen der strategischen Leitlinien das interne und externe Angebot für eine ganzheitliche EDV Unterstützung zur Verfügung.

Ausgehend von den strategischen Zielen der IT beschreibt das vorliegende IT-Konzept die generellen Grundsätze und Voraussetzungen des IT-Angebotes. Neben diesen eher allgemeingültig formulierten Aufgaben und Standards liegt ein konkretes Leistungsangebot vor.

Gleichzeitig wird der technische, organisatorische und z. T. auch rechtliche Rahmen für den Einsatz der Informationstechnologie im Bereich der Evangelischen Landeskirche in Württemberg beschrieben.

3.1. Warum ein IT-Konzept der Evangelischen Landeskirche in Württemberg?

Bereits seit Jahren, sogar Jahrzehnten, wird die kirchliche Arbeit durch den Einsatz der Elektronischen Datenverarbeitung unterstützt und effizienter gemacht. Die Verarbeitung der kirchlichen Gemeindegliederdaten, Programme zur Unterstützung des kirchlichen Haushalts-, Kassen- und Rechnungswesens sowie zur Erstellung der Gehaltsabrechnungen kirchlicher Mitarbeiterinnen und Mitarbeiter bilden neben der Bürokommunikation und der Nutzung des Internets die Schwerpunkte.

Für eine solche Zusammenfassung gibt es interne und externe Anstöße:

- *Regelungsbedarf*

  Die immer komplexer werdenden technischen Rahmenbedingungen machen es notwendig, die tägliche Arbeit im IT-Bereich systematisch zu erfassen und zu ordnen.

  Die Definition von Standards ist ein notwendiger erster Schritt und Vorrausetzung für zukunftsfähige, wirtschaftliche und sichere Anwendung der IT.

- *Zukunftsfähigkeit*

  Um eine EDV-Landschaft systematisch weiterentwickeln zu können, ist es erforderlich, aufeinander abgestimmte Standards einzusetzen, die einen weiteren Auf- und Ausbau zulassen. Eine nicht koordinierte und ungeregelte EDV wirkt als Bremse für den technischen Fortschritt und damit in Zusammenhang stehende Arbeitserleichterungen und Prozessoptimierung. An Stellen, an denen lokale Lösungen existieren, die von Einzelpersonen erstellt und gepflegt wurden, ist eine Vertretung kaum möglich. Bei Weggang der Personen entsteht oft Unsicherheit und meist ist eine grundlegende Neuordnung durch den Nachfolger notwendig.

- *Vereinfachung*

  Standards verringern die Anzahl der Probleme, die sich sonst mit der Menge der betriebenen Systeme und Software und der in Folge daraus entstehenden Schnittstellenvielfalt exponentiell vermehren.

  Durch Nutzung von Standardwendungen kann der ansonsten oft nicht unerhebliche Zeitaufwand für Systemkoordination und Fehlersuche entfallen.

- *Kostensenkung*
  Viele verschiedene Hardware-Systeme und Softwareprogramme mit den damit verbundenen Schnittstellen erfordern zur Pflege vielfältiges EDV-Wissen und viele EDV-Fachkräfte um die Systeme am Laufen zu halten. Dies verursacht erhebliche Kosten, ebenso wie die höhere Anzahl von Schnittstellenproblemen, Fehlinvestitionen in nicht kompatible Hard- und Software sowie unzureichende Kommunikation des EDV-know-hows auf mehrere Personen. Daher ist es sinnvoll, sich auf möglichst wenige, kompatible und einheitlich verwendete Hard- und Softwarekomponenten zu beschränken.

- *Datensicherheit und Datenschutz*
  Die Einhaltung der Datensicherheits- und Datenschutzbestimmungen erfordern heute gewisse Standards (Stichwort: IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnologie) die auch wir als Kirche anwenden müssen.

- *Unterstützung bei EDV-Fragen*

Aber auch in den kirchlichen Dienststellen außerhalb des Oberkirchenrats wurde das Vorhaben, ein IT-Konzept der Evangelischen Landeskirche in Württemberg zu erstellen und zu pflegen, begrüßt. Aus Stellungnahmen der im Vorfeld beteiligten Dienststellen und Verbände kommt der eindeutige Wunsch nach einer weitergehenden Unterstützung bei EDV-Fragen. Von der Pfarrervertretung wurde die Erstellung bzw. Beschreibung von Standards in der IT ausdrücklich begrüßt und gebeten, den Geltungsbereich des Systemkonzepts auf die Pfarrämter zu erweitern. Auch die Vertreter der Kirchlichen Verwaltungsstellen haben sich konstruktiv an der Diskussion beteiligt. Dies zeigt uns deutlich, dass auch in der Fläche ein Bedarf an strategischen Vorgaben und Hilfen zur konkreten Umsetzung besteht.

3.2. Was umfasst das IT-Konzept der Evangelischen Landeskirche in Württemberg?

Neben der umfassenden Auflistung vor allem der technischen Rahmenbedingungen und Standards beim Einsatz von EDV liegen die Schwerpunkte des IT-Konzepts der Evangelischen Landeskirche in Württemberg in den folgenden Bereichen:

- Beschrieben werden die technischen Rahmenbedingungen und Standards beim Einsatz von EDV in der kirchlichen Verwaltung, z. B. für den Aufbau und Betrieb von PC-Netzen, bei der Telekommunikation, für Betriebssysteme etc.

  Beschreibung und Auflistung der Standard-Komponenten und deren Software-Versionen für die Bürokommunikation: Microsoft Exchange mit Outlook (E-Mail und öffentliche Ordner), Word, Excel über den Internet-Zugang und einen PDF-Reader sowie Softwareprodukte, die nicht alle an jedem Arbeitsplatz vorhanden sein müssen (PowerPoint, Microsoft Project, Publisher, Programme zur Datenkomprimierung, ...)

- Beschreibung und Auflistung der übrigen eingesetzten Grundverfahren (Fachsoftware, die einheitlich im gesamten Bereich der Landeskirche zum Einsatz kommt wie z. B. Navision-K, KIDICAP und Personal Office oder die Meldewesenprogramme)

- Ein weiterer Schwerpunkt liegt auf der Sicherheit in der Informationstechnologie (im Bereich der Informationstechnologie im OKR wird die schrittweise Umsetzung der Vorgaben zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnologie angestrebt). Zu diesem Bereich gehören auch der ständig zu aktualisierende Schutz vor Viren, Würmern, Spam-Mails u. a. und der Betrieb einer Firewall zum Schutz von unberechtigten Angriffen von außen.

In weiten Teilen beschreibt das IT-Konzept der Evangelischen Landeskirche in Württemberg dabei die bestehenden Gegebenheiten und fasst die im Einsatz befindlichen Standards (z. B. für den Datenschutz) zusammen. Aufgrund der Größe des OKR-internen Netzes und der Vielzahl der dort im Einsatz befindlichen Programme nimmt die Darstellung und Beschreibung der IT-Landschaft in diesem Bereich einen großen Raum ein.

3.3. Für wen gelten die Regelungen?

Das IT-Konzept der Evangelischen Landeskirche in Württemberg ist eine Verwaltungsvorschrift, die mit Beschluss des Kollegiums vom 28. Juni 2005 in Kraft trat und in regelmäßigen Abständen durch das Dezernat 7 überarbeitet und angepasst wird.

Die Festlegung der Standards beinhaltet i. d. R. keine Entscheidung über Beschaffung und Wartung der EDV. Diese kann sowohl dezentral oder zumindest in Teilen auch zentral erfolgen. Ausnahmen sind zentral betreute Systeme wie im Finanz- und Rechnungswesen die Programme KIFIKOS und Navision-K oder KIDICAP und Personal Office im Bereich Personalwesen.

Verpflichtend
Für den Bereich ELK i. e. S., vorläufig mit Ausnahme der Pfarrämter, sind die Bestimmungen des IT-Konzepts der Evangelischen Landeskirche in Württemberg verbindlich.

Als Empfehlung
Für die Verwaltungen der Kirchengemeinden, die Pfarrämter und die Kirchenbezirke hat das IT-Konzept der Evangelischen Landeskirche in Württemberg empfehlenden Charakter. Damit sollen die Kommunikation in der Landeskirche und die Integration in ein künftiges EDV- Netz der Landeskirche sichergestellt und Fehlinvestitionen vermieden werden.

Um den Bedürfnissen kleinerer Dienststellen zu entsprechen, wird das IT-Konzept der Evangelischen Landeskirche in Württemberg um zwei Anlagen ergänzt, welche die (IT-Konzept der Evangelischen Landeskirche in Württemberg-konforme) mögliche Ausgestaltung der Informationstechnologie vor Ort beschreiben, erforderliche Hard- und Software benennen und an Beispielen die Handhabung anschaulich machen. In diesem Bereich ist Anfang des Jahres 2006 auch die erste Fortschreibung erfolgt.

Service des Referats IT
Das Referat Informationstechnologie in der Landeskirche und im Oberkirchenrat (Ref. 7.4) versteht sich als Dienstleister und bietet den Einrichtungen der Landeskirche auf der Grundlage des IT-Konzepts der Evangelischen Landeskirche in Württemberg Einzelleistungen an, die in der Regel Bereitstellung, Wartung und Beratung beinhalten. Die Umsetzung des Systemkonzepts in diesem Bereich auf Einzelleistungen erfolgt über eine Vereinbarung zwischen den Empfängern von Leistungen und dem Referat IT. Grundlage dieser Vereinbarungen sind die schriftliche Fixierung der Einzelleistungen und deren Kosten aufgrund der Preisliste des Ref. IT (Anlage 3 des IT-Konzepts der Evangelischen Landeskirche in Württemberg).

Dadurch ist eine abgestufte und variable Betreuungsintensität in verschiedenen landeskirchlichen Einrichtungen möglich, die nach Bedarf ausgebaut oder zurückgefahren werden kann. Für bestimmte Programme, etwa im Bereich des Finanz- und Rechnungswesens oder des Personalwesens, bleibt zur Sicherung der Funktionsfähigkeit die zentrale Betreuung obligatorisch.

Eine Ausweitung des Serviceangebots auf Kirchenbezirke und Kirchengemeinden ist perspektivisch denkbar, zurzeit aber noch nicht vorgesehen.

3.4. Was sind die Alternativen?

In anderen Landeskirchen werden zum Teil zentralisiertere Lösungen mit erheblichen Finanzmitteln eingesetzt. So wird z. B. in Hannover eine flächendeckende Vernetzung angestrebt. In Baden wird ein Intranet aufgebaut – damit wurden auch dort viele Standards festgelegt.

Das IT-Konzept der Evangelischen Landeskirche in Württemberg strebt keinen Zentralismus an, möchte aber vermeiden, dass sich eine Vielfalt an EDV-Lösungen, auch Insellösungen, entwickelt, die das Miteinander und die Kommunikation untereinander auf lange Sicht erschweren und die Einführung zukunftsträchtiger Technologien unmöglich oder sehr aufwendig machen würde. Ein solcher Zustand ist auch aus finanzieller Sicht nicht erstrebenswert.

Vielmehr sollte soweit wie möglich auf gemeinsame Lösungen gesetzt werden, wie die Evangelischen Landeskirche das z. B. bei der Personalabrechnung mit KIDICAP und im Bereich Haushalts-, Kassen- und Rechnungswesen mit KIFIKOS schon seit Jahren tut und mit Navision-K in erweiterter Form fortsetzen wird.

3.5. Fortschreibung des IT-Konzepts der Evangelischen Landeskirche in Württemberg

Das IT-Konzept der Evangelischen Landeskirche in Württemberg soll jährlich fortgeschrieben werden, damit der laufenden Entwicklung in der Informations- und Kommunikationstechnologie Rechnung getragen wird.

Das IT-Konzept der Evangelischen Landeskirche in Württemberg und die künftigen Fortschreibungen werden in geeigneter Weise den übrigen Verwaltungen der Landeskirche bekannt gegeben. Die beiden Anlagen zur praktischen Umsetzung in den externen Dienststellen werden ggf. in kürzeren Abständen aktualisiert, wenn dies erforderlich wird.

Die künftigen Fortschreibungen werden in der EDV-Kommission vorgestellt und beraten.

II Rechtliche und organisatorische Vorgaben

Die für die Landeskirche gültigen gesetzlichen Regelungen bezüglich der elektronischen Datenverarbeitung, Datenschutz und Datensicherheit sind hier aufgeführt. Diese Regelungen sind grundsätzlich zu beachten. Im Internet finden Sie die gesetzlichen Regelungen unter http://elk-wue.luchterhand.de/elk-wue/lpext.dll?f=templates&fn=main-h.htm&2.0, bzw. unter http://okrweb.elk-wue.de/datenschutz.

Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG.EKD)
Vom 12. November 1993 (ABl. EKD S. 505) – geändert durch Kirchengesetz vom 7. November 2002 (ABl. EKD S. 381, ber. ABl. EKD 2003 S. 1)

Datenschutzverordnung der Evangelischen Landeskirche in Württemberg
Kirchliche Verordnung zur Durchführung und Ergänzung des Kirchengesetzes über den Datenschutz vom 14. Februar 1995 AZ 11.820 Nr. 103

Datenverschlüsselungsverordnung
vom 20. Dezember 2000 AZ 87.00 Nr. 67

Datensicherungsverordnung
vom 20. Dezember 2000 AZ 87.00 Nr. 67

Computervirenschutzverordnung
vom 20. Dezember 2000 AZ 87.00 Nr. 67

Kirchliches Gesetz über Planung kirchlicher Arbeit, Finanzmanagement und Rechnungswesen in der Evangelischen Landeskirche in Württemberg (Haushaltsordnung)
vom 27. November 2003. (Abl. 61 S. 1)

Richtlinien zum Einsatz der elektronischen Datenverarbeitung
in der Evangelischen Landeskirche in Württemberg
vom 25. März 1997 AZ 87.570 Nr. 70

Ordnung über die Arbeitsbedingungen auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik (Bildschirmordnung)
Beschluss der Arbeitsrechtlichen Kommission vom 22. Juli 1999 (Abl. 58 S. 286)

Kirchliches Gesetz über die Führung von Verzeichnissen betreffend die Gemeindeglieder in der Evangelischen Landeskirche in Württemberg (Kirchenregistergesetz)
vom 8. März 1991 (Abl. 54 S. 543)

– und die dazugehörigen Ausführungsverordnungen –

Synodalbeschluss zur Einführung eines neuen kirchlichen Finanzmanagements und Rechnungswesens
Beschluss der Synode der Evangelischen Landeskirche in Württemberg vom 27. November 2002.

Arbeitsrechtliche Regelung zur Telearbeit -Dienstzimmer im Privatbereich-
Beschluss der Arbeitsrechtlichen Kommission vom 8. Dezember 2006 (Abl. 62 S. 328)

Allgemeine Regelung der Arbeitsabläufe im Oberkirchenrat (Kanzleiverfügung)
Verfügung des Vorstands vom 31. Mai 2001, geändert durch Verfügung des Vorstands vom 15. Juni 2004

III Netz- und Kommunikationsstrukturen

In diesem Abschnitt werden die technischen Vorraussetzungen für eine Vernetzung im IT-Bereich beschrieben. Dabei werden neben der 'klassischen' Technologie mit Verbindungen über physische Leitungen auch die verschiedenen Ausprägungen der neu entstandenen drahtlosen Verbindungstechniken angesprochen. Dieses Kapitel gibt weiterhin Auskunft über die zum Datentransport benötigten Protokolle, ohne die ein sinnvoller Datentransport überhaupt nicht möglich wäre. Außerdem sind die zur Nutzung des Internets notwendigen Protokolle und Dienste beschrieben. Die verwendeten Abkürzungen werden in der Anlage 4 'Abkürzungsverzeichnis' erklärt. Die Beschreibungen all der technischen Voraussetzungen beziehen sich in erster Linie auf das quantitativ und qualitativ breit angelegte Netz im Oberkirchenrat, für kleinere Netzwerke gibt Anlage 1 ausreichende Hinweise.

1. Verkabelung

Um elektronische Informationen und Rechnerleistung am Arbeitsplatz zur Verfügung zu stellen, wird die Versorgung der Arbeitsplätze mit Informationen über das LAN (Local Area Net-work) sichergestellt. Das LAN hat dabei mehrere Dienste (u. a. elektronische Post, Zugriff auf Intranet-Server und auf zentrale Verfahren) zu unterstützen. Ziel einer LAN-Planung in der Evangelischen Landeskirche in Württemberg ist, dass ein LAN anwendungsunabhängig, universell einsetzbar ist und zukünftige Anforderungen ohne größere zusätzliche finanzielle Mittel abdecken kann. Dabei sind die Faktoren Wirtschaftlichkeit und Produktneutralität bei der Planung zu berücksichtigen. Der Umzug von Dienststellen kann kostengünstiger gestaltet werden, wenn die Verkabelung weiterhin genutzt werden kann. In dieser Konzeption wird zur Investitionssicherung zudem eine Aufteilung in einen passiven und einen aktiven LAN-Teil empfohlen.

Den konzeptionellen Rahmen bestimmt die europäische Norm DIN EN 50 173 Stand Juli 2000. Sie beschreibt die strukturierte Verkabelung in Form von anwendungsunabhängigen, universell einsetzbaren Netzkonzepten.

Die Technologie im LAN-Bereich ist schnelllebig. Um einigermaßen mit der neuen Technologie Schritt zu halten, ist vorgesehen, sich künftig an der LAN-Konzeption des Landes Baden-Württemberg zu orientieren. (Siehe LAN-Konzeption der Landesverwaltung Baden-Württemberg http://www.verwaltungsreform-bw.de/servlet/PB/menu/1153853/index.html)

2. Drahtlose Verbindungen

Standard	Beschreibung/Definition	Einsatz/Begründung
Funk-LAN (Wireless LAN) (WLAN)	Funk-LANs bzw. Wireless LANs (WLANs) basieren auf dem vom IEEE definierten Standard IEEE 802.11 und bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen oder bestehende drahtgebundene Netzwerke zu erweitern. Funk-LAN-Systeme gemäß der Erweiterung des Standards 802.11b und 802.11g haben sich mittlerweile am Markt durchgesetzt (Datenrate max. 11-54 Mbit/s, Reichweite zwischen Teilnehmer und Basisstation (Access Point) max. 30-300m). Zurzeit wird ein Standard 802.11n verabschiedet, der Funkübertragungen mit höherer Bandbreite erlaubt. Ein Funk-LAN ist ein Shared-Media-Netz, d.h. mehrere Teilnehmer teilen sich die Übertragungsrate von max. 11Mbit/s. WLANs nach 802.11a mit der Erweiterung 802.11h senden im 5 GHz-Band und erreichen eine Datenrate von max. 54 Mbit/s brutto. Es existiert ein eigenes "eingebautes" Verschlüsselungsprotokoll namens "Wired Equivalent Privacy" (WEP). Mittlerweile wurde dieses Protokoll gemäß IEEE-802.11i zum "Wi-Fi Protected Access" (WPA bzw. WPA2) weiterentwickelt, das höheren Sicherheitsanforderungen entspricht.	Einsatz: Funk-LANs können zur Einbindung mobiler Geräte (auch PDAs) in ein LAN oder für Szenarien ohne verkabelte Räume eine wirtschaftliche Variante zu drahtgebundenen LANs sein. Aufgrund der bequemen Einrichtung der Netze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA oder WPA2 Verschlüsselung einschalten (mindestens 128 bit) • Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
Bluetooth	Bluetooth ist ein Industriestandard (IEEE 802.15.1) für ein lizenzfreies Nahbereichsfunkverfahren zur drahtlosen Sprach- und Datenkommunikation zwischen IuK-Geräten. Im Vergleich zum Funk-LAN (s. o.) hat Bluetooth eine geringere Reichweite (~10m), bietet aber geringe Hardwarekosten, niedrigen Stromverbrauch und Echtzeitfähigkeit in den Bereichen Sprachübertragung und Audio-Video-Lösungen. Bluetooth wird sich voraussichtlich in der drahtlosen Übertragung zwischen Kleinstgeräten durchsetzen und die Datenübertragung mittels Infrarotverbindungen (IrDA) ablösen.	Einsatz: Bluetooth bietet sich für die drahtlose Anbindung von Peripherie-Geräten an stationäre Geräte an. Bei der Kopplung von mobilen Geräten in nicht abhörsicheren Umgebungen sind geeignete Schutzmaßnahmen zu ergreifen (Ausreichend lange PIN, nicht benutzte Dienste abschalten, Verschlüsselung). Näheres siehe Informationsschrift "Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte" (BSI, 2003)

3. Transport-Protokolle

Standard	Beschreibung/Definition	Einsatz/Begründung
TCP/IP IPv4 Internet-Standard	TCP (Transmission Control Protocol) ist ein verbindungsorientiertes Transportprotokoll. Es unterstützt die Funktionen der Transportschicht und stellt vor der Datenübertragung eine Verbindung zwischen den Instanzen her. Das Internet Protocol operiert auf Ebene 3 des OSI-Modells (ist aber nicht zu diesem konform) und sorgt für das Routing (Wegewahl). Es arbeitet verbindungslos und paketorientiert, bietet jedoch keine gesicherte Datagramm-Übergabe. Zu den Standardanwendungen von TCP/IP zählen z. B. Telnet, FTP, E-Mail oder WWW-Anwendungen.	Einsatz: TCP/IP ist das Standard-Basisprotokoll für Ende-zu-Ende-Verbindungen im Netz des OKR und zur Kopplung mit anderen Netzen generell anzuwenden. Die Adresspläne werden beim Referat IT geführt, neue Adressen werden nur vom Referat IT vergeben. Begründung: Bestandteil der einheitlichen IT-Infrastruktur.
TCP/IP IPv6 Internet-Standard	Fundstelle: IPv6 ist eine von der IETF (Internet Engineering Task Force) erarbeitete IP-Protokollversion. Die Version 6 des IP-Protokolls umfasst insbesondere folgende Erweiterungen gegenüber IPv4: • Erweiterte Adressierungsmöglichkeit (128 Bit-Adressen) • Vereinfachung des Headerformates • Neue Möglichkeiten der Dienstgüte • Verbesserte Sicherheitsaspekte (IPsec).	Einsatz: Kurzfristig besteht kein Bedarf in der Landeskirche. Mittel- bis langfristig wird sich der Bedarf entwickeln. Deshalb sollte beim Kauf von Hard- und Software bereits heute aus Gründen der Investitionssicherheit und der Wirtschaftlichkeit die Möglichkeit eines Migrationspfads zu IPv6 gefordert werden.

Standard	Beschreibung/Definition	Einsatz/Begründung
	Die Migration von IPv4 zu IPv6 vollzieht sich vor allem in den Hosts, Routern und Switches. Da die Dauer der Übergangsphase kaum vorhersehbar ist, sollte die Interoperabilität sehr lange gegeben sein. Dazu muss jeder IPv6-fähige Host auch über einen Stack für IPv4 verfügen.	Begründung: Durch die sukzessive Ergänzung der Version IPv4 um wichtige Funktionen von IPv6 ist eine Migration zu IPv6 derzeit noch nicht erforderlich und bei Mehrkosten wirtschaftlich nicht begründbar.

4. Erweitertes Netz des OKR

Standard	Beschreibung/Definition	Einsatz/Begründung
Landeskirchlicher Standard	Unter dem "erweiterten OKR-Netz" werden die bestehenden Netzverbindungen zwischen dem OKR, dem KRZ-SWD und anderen Dienststellen verstanden. Dieses Netz wird durch Verträge über Standleitungen, ATM-DSL, Richtfunkverbindungen und andere Netzverbindungen erstellt. Basis sind Router-Router-Kopplungen und eine einheitliche IP-Struktur. Dadurch können gemeinsam und kostengünstig Ressourcen und Sicherheitstechnologien (z. B. Firewall und Virenschutz) genutzt werden.	Einsatz: Verbindung zum KRZ-SWD Andere Verbindungen (DWW, Medienhaus, Kirchliche Verwaltungsstellen, Haus Birkach, Möhringen, Kirchenpflegen)

5. Anwendungs-Protokolle in Intranets

Die Nachgenannten Protokolle setzen i. d. R. direkt auf TCP/IP auf. Es sollten immer die jeweiligen TCP-Standardports genutzt werden.

Standard	Beschreibung/Definition	Einsatz/Begründung
HTTP	Fundstelle: Die Standardisierung von HTTP obliegt dem W3C (World Wide Web Consortium). HTTP (Hyper Text Transfer Protocol) ist ein allgemeines, statusloses, objektorientiertes Protokoll zur Datenübertragung im Rahmen des World Wide Web (WWW); es dient der Adressierung der Objekte über URL (Uniform Resource Locator), wickelt die Interaktion zwischen Client und Server ab und sorgt für die Anpassung der Formate zwischen Client und Server.	Einsatz: HTTP wird im Verbund des OKR-Netzes und für die Publikation von Informationen im Internet genutzt und auf der Grundlage einer Risikoanalyse eingerichtet und dementsprechend z. B. durch Firewall-Technik gesichert. Begründung: Der Betrieb der Intranets im OKR-Netz ist dem jeweiligen Sicherheitsbedarf entsprechend zu gestalten. Dies gilt im Besonderen auch für Publikation von Informationen im Internet.
HTTPS	Fundstelle: Die Standardisierung von HTTPS obliegt dem W3C (World Wide Web Consortium). HTTPS ist eine sichere Variante von HTTP, die die Dienste von SSL V. 3 (Secure Socket Layer) bzw. TLS V1.0 (Transport Layer Security) nutzt (vgl. Nr. 9.7.2). HTTPS erweitert HTTP um Authentifizierung und Datenverschlüsselung zwischen Web-Server und Web-Browser.	Einsatz: HTTPS wird überall eingesetzt, wo ein gesichertes Kommunikationsprotokoll zwischen Web-Browser und Web-Server notwendig ist. Der Einsatz erfolgt somit bei Bedarf z. B. bei Passwortabfragen, bei der Kommunikation mit dem Portal und in einem Intranet- oder Extranet-Verbund. HTTPS kann bei Bedarf über Intranet-Grenzen (auch zu anderen Intranets) hinweg genutzt werden, ohne dass eine besondere Risikoanalyse erforderlich ist.
		Sofern US-Produkte eingesetzt werden, sind die hoch sicheren Produktversionen zu nutzen bzw. darauf zu migrieren. Begründung:

Standard	Beschreibung/Definition	Einsatz/Begründung
		HTTPS ist besonders geeignet, die Integrität, die Vertraulichkeit und die Authentizität der Kommunikation zwischen Web-Browser und Web-Server auf einfache und wirtschaftliche Weise sicherzustellen. HTTPS ist Bestandteil der einheitlichen IT-Infrastruktur
MIME	MIME (Multipurpose Internet Mail Extension) stellt eine Erweiterung des Internet E-Mail-Standards SMTP (RFC 822) dar, um wie bei X.400 beliebige Dateien wie Grafiken, Verbunddokumente, Tabellenkalkulationen, Sprachdateien, etc. als sog. Attachments auch per SMTP versenden zu können. Voraussetzung für den richtigen Empfang und die korrekte Darstellung dieser multimedialen elektronischen Post ist, dass das Mail-Programm des Empfängers ebenfalls den MIME-Standard und die entsprechenden Dateiformate unterstützt.	Einsatz: Für den elektronischen Austausch von beliebigen Dateiformaten per SMTP Begründung: MIME ist beim vollwertigen Einsatz von SMTP in der Verwaltung zwingend erforderlich.
S/MIME	S/MIME ist ein Protokoll, um den E-Mail-Versand mit SMTP/ ESMTP und MIME durch elektronische Signatur und Verschlüsselung zu sichern.	Wo die Wahl besteht, ist das sicherere S/MIME V3 dem S/MIME V2 vorzuziehen.
LDAP	Fundstelle: insbesondere RFC 2251 (LDAP V. 3) LDAP (Light Weight Directory Access Protocol) ist ein Standard der Internet Engineering Task Force (IETF). LDAP spezifiziert den interaktiven Zugriff (lesend und schreibend) auf Verzeichnisse, die dem X.500-Modell entsprechen. LDAP ist speziell ausgerichtet auf Management-Anwendungen und Benutzer-Zugriffe über Browser und kann auch für den Zugriff auf standardkonforme X.500-Verzeichnisse eingesetzt werden. Aktuell ist die Version 3, die u. a. eine wesentliche Komponente der Active Directory Services von Windows 2000/2003 ist.	Einsatz: LDAP hat in der kirchlichen Verwaltung durch den Einsatz des Active Directory, zentrale Bedeutung. Der Einsatz von LDAP ist im Intranet-Verbund mit anderen Netzen ohne besondere Risikoanalyse zulässig. Begründung: Die generellen Sicherheitsmaßnahmen des Referats IT für die zentralen Dienste des OKR-Netzes sind ausreichend. LDAP ist Bestandteil der einheitlichen IT-Infrastruktur
DNS	DNS (Domain Name Service) ist ein Dienst/ Protokoll, der für einen logischen Rechnernamen (z. B. in Form der URL) die IP-Adresse des Rechners bereitstellt. Bei Windows 2000/2003 ist DNS als integrierter Dienst zur IP-mäßigen Lokalisierung von Active Directory Computerobjekten innerhalb einer AD-Domainstruktur implementiert.	Einsatz: DNS hat in der Kirchlichen Verwaltung durch den Einsatz von Windows 2000/2003 Active Directory Services im Rahmen von ressortübergreifenden Netzwerk-Anwendungen zentrale Bedeutung und ist zwingend erforderlich.
FTP	Das FTP (File Transfer Protocol) dient dem Dateitransfer zwischen verschiedenen Systemen und der einfachen Dateihandhabung. FTP eignet sich für die Übertragung sowohl zeichencodierter Information als auch von Binärdaten.	Einsatz: FTP wird im Intranet-Verbund des OKR-Netzes nur auf der Grundlage einer Risikoanalyse eingerichtet und dementsprechend insbesondere durch Firewall-Technik gesichert. Begründung: FTP stellt ein besonderes Sicherheitsrisiko dar*. *) Passwörter und Kommandos werden bei FTP im Klartext übertragen. Beim Unix- /Linux-basierten SSH (Secure Shell) wird dagegen verschlüsselt/signiert, so dass dies im Bedarfsfall bevorzugt werden sollte.
TELNET	Das Telnet-Protokoll erfüllt die Funktion des virtuellen Terminals. Es ermöglicht den Fernzugriff vom eigenen Arbeitsplatz-Rechner auf andere im Netzwerk befindliche Computersysteme, Router, etc.. Telnet ermöglicht eine bidirektionale Kommunikation, um Datenendgeräte mit entsprechenden Prozessen zu verbinden.	Einsatz: Telnet wird im Intranet-Verbund des OKR-Netzes nur auf der Grundlage einer Risikoanalyse eingerichtet und dementsprechend insbesondere durch Firewall-Technik gesichert. Telnet stellt ein besonderes Sicherheitsrisiko dar.
NNTP	NNTP (Network News Transfer Protokoll) regelt den regelmäßigen Austausch von News zwischen zwei NNTPServern und spezifiziert interaktive Kommandos für die Kommunikation	Einsatz: NNTP wird im Intranet-Verbund des OKR-Netzes nur auf der Grundlage einer Risikoana-

Standard	Beschreibung/Definition	Einsatz/Begründung
	zwischen News-Clients und News-Server. Die Wirkung von NNTP ähnelt der von SMTP, nur werden keine interpersonellen Nachrichten sondern Artikel (sog. Postings) übertragen.	lyse eingerichtet und dementsprechend insbesondere durch Firewall-Technik gesichert.
SMTP/ESMTP	Fundstelle: RFC 821, RFC 1869 u. a. Hierzu relevante Standards: • Post Office Protocol V. 3 (POP 3): RFC 1018 • Internet Mail Access Protocol (IMAP): RFC 1730 und 2030 • MIME (siehe oben) Das SMTP (Simple Mail Transfer Protocol) ggf. mit der Erweiterung "Enhanced SMTP (ESMTP)" ist der Internet-Standard zum Versenden/Verteilen von E-Mails. Der Abruf der E-Mails aus den Postfächern durch die Mail-Clients erfolgt i. d. R. über RPC (bei Client-Server-Systemen im LAN). An die Mail angehängte Dateien (sog. Attachments) werden bei SMTP in das MIME-Format konvertiert. ESMTP bietet folgende zusätzlichen Funktionen zu SMTP: • 8-bit Zeichensatz • die Meldung von Teilnehmern bzw. das direkte Feedback, ob eine Mail erfolgreich zugestellt wurde • weitere, beim Aufbau der Verbindung individuell ausgehandelte Funktionalitäten. SMTP wird auch als Standardprotokoll für die Verzeichnisreplikation im Windows 2000/2003 Active Directory Service verwendet.	Einsatz: (siehe auch Nr. V.2.1) ESMTP wird im OKR-Netz als ein zu X.400 bevorzugter Standard eingesetzt. Der Einsatz von SMTP/ESMTP ist im Intranet-Verbund des OKR-Netzes ohne besondere Risikoanalyse zulässig. Begründung: Nur mit ESMTP kann eine mit MHS X.400 vergleichbare Dienstgüte von SMTP erreicht werden.
SNMP	Fundstelle:RFC 1052, RFC 1155, RFC 1156, RFC 1157, RFC 1213 und RFC 1441. Das SNMP-Protokoll (Simple Network Management Protocol) spezifiziert die Kommunikation zwischen der Managementstation und den daran angeschlossenen Systemen im Netz, die über sog. SNMP-Agenten verfügen. Diese Kommunikation umfasst die Übertragung z. B. von Fehlermeldungen und relevanten Statistiken, die entsprechend der Definition in der sog. Management Information Base (MIB) in den Systemen gesammelt werden, zur Managementstation und umgekehrt der Generierungsdaten zu den zu administrierenden Systemen.	Einsatz: zur Administration und Überwachung von beliebigen Komponenten in einem TCP/IP-Netzwerk Begründung: Das SNMP-Protokoll in der Version 2.0 ist erforderlich für ein zentrales Netzwerk- und Systemmanagement. Die Überwachung von Servern- und Netzwerkkomponenten in der Kirchlichen Verwaltung erfolgt durch SNMP-Agenten, die bei vorgegebenen Schwellenwerten, Fehlern oder Ereignissen mittels SNMP eine Mitteilung direkt an die System-Monitoring-Datenbank senden. System-Monitoring kann bei entsprechender Konfiguration diese Mitteilung an das Problemmanagement HELPLINE weiterleiten.
SNTP, NTP	Fundstelle: RFC 1769 (SNTP), RFC 1305 (NTP) u. a. Das SNTP-Protokoll (Simple Network Time Protocol) wird für die Übertragung einer offiziellen Uhrzeit in Netzwerken und im Internet verwendet. Das SNTP-Protokoll zeichnet sich durch Einfachheit aus, hat dafür allerdings eine Ungenauigkeit im Bereich von mehreren hundert Millisekunden. NTP (Network Time Protocol) liefert eine genauere Zeitangabe als SNTP. NTP wird durch synchronisierte Time-Server, die sich an verschiedenen Punkten im Internet/Intranet befinden, realisiert. Die resultierende gemeinsame Zeitbasis wird für Applikationen wie z. B. Authentifizierungssysteme benutzt.	Einsatz: NTP wird zur Zeitsynchronisation von Servern und Clients im OKR-Netz eingesetzt Begründung: Das NTP -Protokoll ist ein Standard-Dienst
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol (SOAP) hat das Ziel, den Austausch von strukturierter Information zwischen verteilten, dezentralisierten Rechnern zu standardisieren. Dazu benützt es ein Protokoll, welches auf XML basiert. Die SOAP Spezifikation beinhaltet drei wichtige Bereiche:	Einsatz: Überbrückung der Heterogenität von Anwendungen durch einen plattform- und programmiersprachenunabhängigen Mechanismus zur Kommunikation zwischen Anwendungen, insbesondere auch zur Einbindung von Anwen-

Standard	Beschreibung/Definition	Einsatz/Begründung
	• SOAP definiert einen flexiblen Aufbau der SOAP-Nachricht (d.h. des XML-Dokuments), welcher als "Envelope" bezeichnet wird. • SOAP bietet einen Serialisierungs-Mechanismus, welcher die Umwandlung von Datentypen in XML regelt. • SOAP beinhaltet einen Mechanismus für den Aufruf von entfernten Methoden (RPCs). SOAP ist derzeit in Version 1.2 vom W3C veröffentlicht.	dungen in Web-Services. Generell zum Aufbau einer Service-Orientierten Architektur (SOA)

6. www-Browser zur Nutzung und Gestaltung von Netzwerk-Anwendungen

Standard	Beschreibung/Definition	Einsatz/Begründung
• Microsoft Internet Explorer • Firefox (Open-Source-Ableger u. Weiterentwicklung des ehemaligen Netscape-(Mozilla) Browsers)	Web-Browser sind Client-Programme zur Darstellung und dynamischen Verarbeitung von Web-Seiten im Internet/Intranet. Der Browser ermöglicht das Betrachten der verschiedenen Dokumente im Hypertext-Format und die Navigation zwischen den Dokumenten. Web-Browser sind deshalb Grundlage für den Benutzerzugriff auf Netzwerk-Anwendungen. Die Landeskirche setzt im Bereich der IT-Infrastruktur im erweiterten Netz des Oberkirchenrats hierbei die Produkte von Microsoft (Internet Explorer) ein. Deshalb müssen alle Netzwerk-Applikationen in der kirchlichen Verwaltung der Landeskirche Württemberg so geschrieben sein, dass sie vom Microsoft Internet Explorer genutzt werden können. Außerhalb der einheitlichen IT-Infrastruktur (im Umfeld von UNIX und LINUX) kann der Browser von Netscape/Mozilla eingesetzt werden.	Einsatz: Von den Firmen-Standards werden grundsätzlich nur die Funktionen genutzt, die sich möglichst nahe am HTML/SGML-Standard (s.V 3.5) orientieren. Damit soll soviel Herstellerunabhängigkeit wie möglich erzielt werden. Sämtliche Funktionen sind zugelassen, soweit sie von den genannten Browsern unterstützt werden, also insbesondere • digital signierte Applets • https • Download von Daten • Bürokommunikations-Komponente. Begründung: Bestandteil der einheitlichen IT-Infrastruktur

7. www-Server

WWW-Server können in einer Vielzahl von Techniken realisiert werden. Redaktionssysteme, selbst programmierte IT-Anwendungen sind geeignet und sollen – wo sachgerecht – genutzt werden. Entsprechend kann die funktionale Bandbreite von WWW-Servern von klassischen, "einfachen" HTTP-Servern mit statischen HTML-Seiten zu komplexen Applikations-Servern als sog. Servlet-Engines reichen. Die nachfolgenden Standards gelten für die klassischen WWW-Server. Der Einsatz von Applikations-Servern und die diesbezüglichen Produktentscheidungen werden jeweils im Einzelfall mit dem Referat IT abgestimmt. Hierbei sind insbesondere die Anforderungen zu berücksichtigen, die sich ggf. aus einer möglichst wirtschaftlichen und technisch hochwertigen Anbindung an die Portal-Lösung der Landeskirche ergeben.

Als Kenngröße zur Ermittlung der Zahl der Besuche der Internet-Auftritte kommen die "visits" (auch Sessions (deutsch *Besuche*)) zum Einsatz. "Visits" zählen einen zusammenhängenden Besuchsvorgang etwa im Sinne einer aktiven "Session". Jedes Mal wenn ein Besucher mit einer neuen IP-Adresse die Web-Site erfolgreich aufruft, wird ein zusätzlicher Visit verzeichnet. Da viele IP-Adressen dynamisch vergeben werden, wird nach einer Stunde eine IP-Adresse wieder als neu angesehen. Die Zahl der visits (Besuche) einer Webseite darf nicht mit der Zahl der "unique visitors" (unterschiedliche Besucher) verwechselt werden. Letztere könnte nur mit großem Aufwand ermittelt werden, indem Zugriffe nur nach vorheriger Registrierung und Anmeldung über User/Passwort erfolgen.

Standard	Beschreibung/Definition	Einsatz/Begründung
Internet Information Server bzw. Internet Information Service	Der Internet Information Server (IIS) ist ein Software-Produkt der Firma Microsoft und Bestandteil der Server-Betriebssysteme Windows 2000 bzw. 2003, sowie von Windows XP Professional, und bietet einen WWW-, FTP-, SMTP- und NNTP-Serverdienst an.	Einsatz: Einsatz innerhalb der einheitlichen IT-Infrastruktur, dabei ist die IIS Version 6.0 (integriert in Windows 2003 Server) wegen der höheren Sicherheitsstandards zu bevorzugen. Begründung: keine zusätzliche Hard-/Softwarebeschaffung erforderlich, hohe Verbreitung.
Apache	Bei Apache handelt es sich um einen Web-Server, der unter Open Source License verfügbar ist.	Einsatz: Der Einsatz ist generell zulässig. Im OKR wird Apache hauptsächlich für Internet Web-Server eingesetzt (z. B. Landeskirchliches CMS). Begründung: hohe Verbreitung, Marktführer, Open Source

8. Basisdienste des Webservers

Standard	Beschreibung/Definition	Einsatz/Begründung
ASP Firmen-Standard (Microsoft)	ASP ist die Abkürzung für "Active Server Pages". MS-ASP ist eine Technik zur Einbettung von serverseitig ausgeführten Skripten in HTML-Seiten. MS-ASP kann im Prinzip mit verschiedenen Skriptsprachen kombiniert werden, wird aber fast nur mit VBScript verwendet. Fast alle Beispiele und Dokumentationen setzen VBScript voraus. Da VBScript alleine nicht mächtig genug ist, wird komplexerer Code in COM- oder ActiveX-Komponenten verlagert. Die Microsoft-ActiveX-Library ist nur unter Windows mit dem Microsoft Internet Information Server (IIS) verfügbar. Im Nachfolger von MS-ASP, dem neuen ASP.NET, kommt	

Standard	Beschreibung/Definition	Einsatz/Begründung
	nicht mehr VBScript zur Anwendung. Es können theoretisch alle .NET-Programmiersprachen eingesetzt werden. In den üblichen Dokumentationen und Beispielen wird Visual Basic .NET und C# verwendet.	
PHP	PHP ist eine Skriptsprache die von einem Interpreter ausgeführt wird, der entweder als eigenständiges Programm oder als Modul installiert wird. PHP verfügt über sehr weitgehende Funktionen und ermöglicht damit komplexe Anwendungen mit geringem Aufwand zu entwickeln. PHP ist sowohl für Windows als auch für Linux verfügbar.	Einsatz: Im OKR wird PHP für Webanwendungen eingesetzt (z. B. CMS). Begründung: Einfache Programmierung und leichte Anpassung bestehender Anwendungen

9. Portal

Mit zunehmender Verbreitung der EDV werden immer mehr Informationen digital verfügbar. Um einen Effizienz-Gewinn aus diesem Wandel zu erzielen ist es notwendig diese Informationen den Nutzern auf elektronischem Wege zur Verfügung zu stellen.

Hierfür gibt es verschiedene Möglichkeiten mit entsprechenden Vor- und Nachteilen. Da die Infrastruktur zunehmend günstiger wird, ersetzt diese in weiten Bereichen den Versand von Datenträgern. Zudem ermöglicht dies eine zentrale Datenhaltung mit weniger Redundanzproblemen und einer größeren Aktualität.

Für die Bereitstellung der Informationen wird häufig ein Portal verwendet. Dieses bietet dem Benutzer einen zentralen Zugang zu einer Vielzahl von Informationen. Dieser Zugang kann sowohl authentifiziert als auch personalisiert erfolgen. Meist wird dies mit einem auf Web-Technologien basierenden System realisiert, um möglichst vielen Systemen den Zugriff zu ermöglichen.

Die Datenbasis bilden meist viele verschiedene Systeme aus denen das Portal die Informationen für den jeweiligen Benutzer zusammenstellt. Um die Anzahl der Schnittstellen, und damit auch der Probleme zu reduzieren, empfiehlt es sich die Daten in möglichst wenigen Systemen zu konsolidieren. Diese sollten offene Schnittstellen haben, die einen Import von Daten anderer Systeme ohne allzu großen Aufwand zu ermöglichen. Vor allem für Daten die wenig oder keine Änderungen mehr erfahren werden häufig Archivierungssysteme verwendet.

Im Oberkirchenrat werden viele statische Daten erzeugt, wie zum Beispiel Rundschreiben, Amtsblätter, Formulare und andere Veröffentlichungen. Des Weiteren entstehen in den vom Oberkirchenrat betreuten Systemen Ausgabe-Daten, die elektronisch archiviert werden müssen. Um dem Nutzer diese Datenmengen einfach nutzbar zur Verfügung zu stellen, empfiehlt sich ein System, das die Daten mit Metainformationen versieht und strukturiert ablegt. Zudem ist eine gute Suchmaschine über diese Daten unerlässlich.

9.1. CITRIX-Portal

Um auch nicht webfähige Anwendungen wie zum Beispiel Navision K oder Outlook sicher und benutzerbezogen über das Internet zur Verfügung stellen zu können, wird das von der Firma Citrix stammende Web-Interface in Kombination mit dem Secure Gateway eingesetzt. Damit kann ein Nutzer native Windowsanwendungen über das Internet verwenden ohne diese bei sich installiert haben zu müssen. Vorraussetzung für die Nutzung ist eine Internetanbindung mit ausreichender Bandbreite; ein Offline-Betrieb ist zurzeit nicht möglich.

Standard	Beschreibung/Definition	Einsatz/Begründung
Citrix Secure Gateway mit Web-Interface	Dieses System der Firma Citrix ermöglicht es Terminal-Server Sitzungen über eine SSL-Verbindung Nutzern mit Internetanschluss zur Verfügung zu stellen. Zur Nutzung wird auf Client-Seite lediglich ein Webbrowser benötigt.	Einsatz: Für sämtlich Clients außerhalb des OKR die eine Internet-Anbindung haben aber keinen VPN-Router, z. B. für die flächendeckende Nutzung von Navision. Begründung: Einfachere Administration, größere Freiheit bei der Auswahl der Internetanbindung der Dienststelle

10. Standardisierung von IP-QoS

Zur Erhöhung der Ausfallsicherheit in Netzwerken, zur Integration von Diensten wie Voice over IP, Videoconference over IP etc. in Datennetze und zur Optimierung von Arbeitsgruppen innerhalb einer Netzwerkarchitektur sind nachfolgende Standards aus Gründen der Investitionssicherheit und der Wirtschaftlichkeit bei der Beschaffung von aktiven Komponenten (Switch, Router) zu berücksichtigen.

Standard	Beschreibung/Definition	Einsatz/Begründung
Einrichten von Prioritäten (Quality of Service - QoS)	Durch QoS-Funktionalitäten wird im LAN sichergestellt, dass Sprache vor Daten priorisiert zum Voice Gateway oder zu einem anderen IP-Telefon im LAN übermittelt wird. Die Priorisierung ist insbesondere für Voice over IP und Videoconference over IP erforderlich. Überdies können auch unternehmenskritische Daten gegenüber weniger kritischen priorisiert werden. Zu den Layer-3 QoS-Signalisierungswerkzeugen gehören • das Resource Reservation Protocol (RSVP) und • die IP Precedence. Das Ressource Reservation Protocol dient der Reservierung von Ressourcen in den Routern/ Switching-Komponenten in einem Netzwerk. RSVP baut zuerst einen Pfad über die Router/Switching-Komponenten auf und reserviert in den Routern/Switching-Komponenten die entsprechenden Ressourcen für die nachfolgende Übertragung, die nach Verkehrsklassen unterschieden werden kann.	Einsatz: in Router und Switching-Komponenten zur Priorisierung von Datenpaketen

11. Standards für Telekommunikation

Die herkömmlichen TK-Anlagen werden schrittweise um Voice over IP–Technologie ergänzt. Nachfolgend sind insbesondere Standards für die herkömmliche Telefonie aufgeführt.

11.1. Signalisierung

Standard	Beschreibung/Definition	Einsatz/Begründung
DSS 1 (Euro ISDN) de-facto-Standard	Fundstelle: ITU-T I.411; ETS 300 102 (European Telecommunication Standard) DSS 1 (Digital Subscriber Signaling System No.1) ist ein europäisches ISDN-Protokoll für den D-Kanal. Dieses Protokoll wird einheitlich als DSS1 bezeichnet.	Einsatz: bei digitalen TK-Anlagen der Kirchlichen Verwaltung, die insbesondere mit den Vermittlungssystemen der öffentlichen Telefon-Netzbetreiber gekoppelt sind Begründung: Zukunftssicherheit: In Europa haben sich die meisten Netzbetreiber in fast allen europäischen Staaten zu der Einführung des DSS1 verpflichtet.

11.2. Software/Schnittstellen

Standard	Beschreibung/Definition	Einsatz/Begründung
Voice over IP de-facto-Standard	Voice over IP (VoIP) bezeichnet einen digitalen Sprachdienst über IP-Netze. Die Sprache wird digitalisiert und per Hard- oder Software komprimiert übertragen (siehe auch Nr. 3.3). Der Einsatz von VoIP ist insbesondere wirtschaftlich, wenn Softphones (PC mit Audio-Karte und –Boxen und einer Telefoniesoftware) und Universal-Messaging genutzt werden. Ergonomische Geräte sind am Markt verfügbar. Kleinere Defizite dieser Technik bestehen praktisch nur noch bei speziellen Funktionen wie z. B. der Chef-/Sekretärinnen-Funktion.	Einsatz: Der Einsatz erfolgt in Pilotprojekten. Vor der Beschaffung einer neuen TK-Anlage ist zu prüfen, ob VoIP eine wirtschaftlich günstigere Lösung darstellt. Insbesondere dort, wo sich die Struktur häufig ändert, oder spezielle Funktionen benötigt werden lohnt sich der Einsatz von VoIP. Verträge über herkömmliche TK-Anlagen mit mehr als 5 Jahren Laufzeit müssen dabei besonders geprüft werden. Künftig: Die Ausweitung von VoIP in der Kirchlichen Verwaltung hängt insbesondere ab von • den Ergebnissen der Pilotprojekte • dem Fortgang der Standardisierung und Realisierung im Bereich der QoS (Quality of Services) • der Verbreitung am Markt und der daraus sich entwickelnden Wirtschaftlichkeit. Begründung: Die Wirtschaftlichkeit muss sichergestellt werden.

IV Hardware und Betriebssysteme

In diesem Abschnitt werden Hardware und Betriebssysteme beschrieben. Hardware umfasst die ganze Palette an Gerätschaften, angefangen vom eigentlichen PC mit Bildschirm und Tastatur bzw. Maus bis hin zu den Peripheriegeräten, die für einen ordnungsgemäßen, d. h. zuverlässigen und sicheren EDV-Betrieb unerlässlich sind.

Bezüglich der direkten Nutzung der einzelnen PCs wird zwischen dem persönlichen Arbeitsplatzrechner (Client), den gemeinsam genutzten Rechnern (Server) und den Netzwerkkomponenten (z. B. Router, Switche...) unterschieden.

Betriebssysteme sind Programme (Software), die notwendig sind, damit die eingesetzte Hardware mit den vorgesehenen Programmen wie z. B. eine Textverarbeitung überhaupt funktioniert. Mit Hilfe der Betriebssysteme werden die eingesetzten Komponenten koordiniert und für die verschiedenen Aufgaben zur Nutzung bereitgestellt.

Auch hier ist die Beschreibung sehr breit angelegt, um die im Bereich des Netzes innerhalb des Oberkirchenrats und der angeschlossenen Dienststellen eingesetzten Geräte und Systeme einzubeziehen. Für Einzel-PCs und kleine Netzwerke genügen die in Anlage 1 beschriebenen Komponenten.

1. Hardware-Standards

In der Kirchlichen Verwaltung soll grundsätzlich so leistungsfähige Hardware beschafft werden, dass ein produktiver Einsatz über mindestens 4 Jahre möglich ist. Allerdings kann Hardware vorher ausgetauscht werden, wenn dies nach einer Wirtschaftlichkeitsrechnung haushaltswirksame Vorteile ergibt.

Standard	Beschreibung/Definition	Einsatz/Begründung
Client		
Standard-Client Landeskirchlicher Standard	Ausstattungsmerkmale: • PC mit Intel oder Intel-kompatiblem Prozessor • Grafikkarte • Netzwerkkarte • serieller und paralleler Port • USB-Port (Universal Serial Bus) • Festplatte • Maus und Tastatur • Bildschirm entsprechend der Bildschirmarbeitsplatzverordnung • Powermanagement • CD-ROM-/DVD-Laufwerk und Diskettenlaufwerk, sofern Wirtschaftlichkeits-oder Sicherheitsgründe nicht entgegen stehen • Soundkarte etwa beim Einsatz des PC als Softphone Bei Einsatz von Windows müssen die PC der von Microsoft veröffentlichten Hardware Compatibility List (HCL) entsprechen.	Einsatz: Standard-Arbeitsplatzrechner insbesondere im Kernbereich der einheitlichen Bürokommunikation im Netz des OKR, ggf. mit Integration von Fachanwendungen. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Notebook, Handheld, Blackberry	Mobile Geräte dienen der Rationalisierung, indem insbesondere im Bürokommunikations-System Terminabstimmungen getroffen werden, Passworte sicher gespeichert, Vermerke und Besprechungsprotokolle während Telearbeit (z. B. der Reisezeit etwa im Zug) oder direkt in Besprechungen erstellt, umfangreiche Dokumente und Adressverzeichnisse elektronisch in Besprechungen und auf Dienstreisen mitgenommen und Präsentationen umweltschonend elektronisch vorgeführt	Der Einsatz mobiler Geräte ist i. d. R. wirtschaftlich. Bei der Beschaffung ist zu prüfen, ob ein Gerät für mehrere Mitarbeiter genutzt wird, ob es als Ersatz für einen stationären PC benutzt wird und wie seine Nutzungsdauer erhöht werden kann.

Standard	Beschreibung/Definition	Einsatz/Begründung
	werden können. Mobile Geräte sollen so hochwertig ausgestattet beschafft werden, dass bezogen auf den jeweiligen Anwendungsfall eine möglichst lange Nutungsdauer gewährleistet ist. Vor allem sind Hauptspeicher und Platte so hochwertig zu beschaffen, dass alle in absehbarer Zeit notwendigen Office-, Projekt- Management-, Präsentations- und Fachprogramme darauf problemlos installiert und genutzt werden können. Für Notebooks bieten Dockingstationen mit Tastatur und Monitor für das ergonomische Arbeiten am Arbeitsplatz eine besonders wirtschaftliche Alternative zu normalen Arbeitsplatz- PC. Allerdings ist es in bestimmten Anwendungsfällen nach wie vor sinnvoll, die mobilen Geräte so einzurichten, dass nur wenige Arten des Informationsaustauschs möglich sind, denn dadurch werden Integrationsprobleme vermieden und die Nutzungsdauer erhöht.	Zur Datensicherheit bei mobilen Geräten vgl. das Kapitel IX über Datenschutz und Datensicherheit.
Server		
	Ausstattungsmerkmale: • 32/64-Bit-Rechner • Server müssen bei Beschaffung durch Zusatzprozessoren oder durch stärkere Prozessoren auf mindestens die doppelte Leistung aufgerüstet werden können. • Redundante Bauteile (Netzwerkkarten, Stromversorgung, Festplatten) für höhere Verfügbarkeit • ECC-Speichermodule • RAID-Systeme für DAS • Clusterfähigkeit • Aufrüstbarkeit für SAN-Integration	Einsatz: Standard-Server insbesondere im Kernbereich der einheitlichen Bürokommunikation im Netz des OKR, ggf. mit Integration von Fachanwendungen Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Speicher-Subsysteme SAN		
	Die Trennung von Server (Anwendung) und Speicherfunktion ist das tragende Konzept eines SAN (Storage Area Network). Die Speichermedien werden dabei zentralisiert an ein Netzwerk gekoppelt und sind gleichberechtigte Komponente der Gesamtstruktur. Vorteile: • hohe Performance und Verfügbarkeit • zentralisierte und konsolidierte Speicherung für heterogene Systeme • einfaches und zentrales Management • verbesserte Backup/Recovery Strategien • leistungsfähige Disaster Recovery Prozeduren Ein SAN (Storage Area Network) ist ein Hochgeschwindigkeitsnetzwerk zwischen Servern (Hosts) und Speichersubsystemen. Dabei ermöglicht ein SAN eine any-to-any Verbindung durch das gesamte Netzwerk. Die traditionellen dedizierten Verbindungen zwischen Servern und Subsystemen (DAS/Direct Attached Storage) werden eliminiert. Die Speichersubsysteme werden innerhalb eines SAN unabhängig von den Servern und damit von den eingesetzten Plattformen, das heißt ein einzelnes Speichersubsystem kann einem oder mehreren Servern zugeordnet werden. In einem SAN können sowohl Server als auch Subsysteme große Daten mengen mit großer Geschwindigkeit austauschen. Für den Datenaustausch können u. a. das Fibre-Channel (FC)- oder iSCSI-Protokoll eingesetzt werden. FC erfordert spezielle Hardwarekomponenten und ist dadurch kostenintensiver, aber allgemeinen (noch) leistungsfähiger. Für iSCSI kann hostseitig dagegen eine Standardnetzwerkkarte verwen-	Einsatz: SAN-Systeme (HBA, Platten, Switches, Bandlaufwerke) werden im OKR-Netz grundsätzlich für alle Kernbereiche der Datenspeicherung und im Clusterumfeld eingesetzt. Sowohl das FC- als auch das iSCSI-Protokoll werden verwendet. Begründung: • hohe Geschwindigkeit • Skalierbarkeit • Flexibilität • vereinfachtes Speichermanagement • Sicherheit • hohe Verfügbarkeit • Clusterunterstützung

Standard	Beschreibung/Definition	Einsatz/Begründung
	det werden. Auf der Seite der Speichersubsysteme sind hier auch kostengünstigere Komponenten als im FC-Umfeld möglich. Die Speichersubsysteme selbst verfügen über die gängigen RAID-Technologien.	
Router	Router sind stark spezialisierte Rechner deren einzige Aufgabe es ist den Datenverkehr zwischen einzelnen Computer-Netzwerken zu steuern. Im OKR werden hierfür Produkte der Firma Cisco eingesetzt.	Einsatz: Überall dort. wo Netze gekoppelt werden müssen. Z. B. die Anbindung von Dienststellen an ein Rechenzentrum per ISDN oder via Internet und VPN sein. Ebenso bei der Kopplung einzelner Netz mit Standleitungen. Begründung: Strukturieren der Netzwerke und Eingrenzen des Datenverkehrs auf die betroffenen Netzwerke.
Switches und Hubs	Switches und Hubs stellen die Verbindung zwischen Rechnern und anderen Netzwerkgeräten her. Durch Schalten von gezielten dynamischen Verbindungen zwischen angeschlossenen Geräten erzielen Switches wesentlich höhere Durchsatzraten im Vergleich zu Hubs. Da Switches nur unwesentlich teurer sind, haben diese Hubs vom Markt verdrängt. Bei Switches unterscheidet man zwischen 'managed Switches' und 'unmanaged Switches'.	Einsatz: Überall dort wo mehr als zwei Netzwerkgeräte/ Rechner miteinander verbunden werden sollen. 'Managed Switches' werden vor allem in größeren Netzwerken eingesetzt, um die Verwaltung der Netzwerke zu vereinfachen und ihre Sicherheit zu erhöhen.
Firewall	Aufgabe einer Firewall ist es Computernetzwerke zu schützen. Sie filtern den Datenverkehr und beschränken diesen auf das für die Funktionalität Notwendige.	Einsatz: Überall dort wo Netze miteinander gekoppelt sind und der Datenverkehr geregelt werden muss; z. B. Internetanbindung von Computernetzwerken Begründung: Firewalls schützen die hinter ihnen liegenden Netzwerke vor nicht gewollten Zugriffen Unbefugter.
Monitore		
Ergonomische Anforderungen	Anforderung an Bildschirmgeräte: • Die Zeichen müssen scharf, deutlich und ausreichend groß sein sowie einen angemessenen Zeichen- und Zeilenabstand haben. • Das dargestellte Bild muss stabil und frei von Flimmern sein; es darf keine Verzerrungen aufweisen. • Die Helligkeit der Bildschirmanzeige und der Kontrast zwischen Zeichen und Zeichenuntergrund auf dem Bildschirm müssen einfach einstellbar sein und den Verhältnissen der Arbeitsumgebung angepasst werden können. • Der Bildschirm muss frei sein von störenden Reflexionen und Blendungen. • Das Bildschirmgerät muss frei und leicht drehbar und neigbar sein.	Einsatz von 17-Zoll-Monitoren bei Arbeiten vorwiegend unter Windows oder einer anderen grafischen Benutzeroberfläche sowie bei Navision-K-Anwendern Für CAD-, Layout- und Grafikarbeitsplätze sind mindestens 20- Zoll-Bildschirme zu empfehlen. Begründung: Ordnung über die Arbeitsbedingungen auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik (Bildschirmordnung vom 22.07.1999)
TCO de-facto-Standard	Fundstelle: TCO (Tjänstemännens Central-Organisation) berücksichtigt die Anforderungen der MPR II-Norm. Das Label stellt eine Empfehlung hinsichtlich Ergonomie, Energieverbrauch, Emission und Ökologie von Monitoren, PC und Tastaturen dar. Nach TCO 92, TCO 95 und TCO 99 wurden mit dem TCO 2003 die Standards für die technischen Geräte noch weiter angehoben: • Alle TCOs verlangen jeweils Verbesserungen hinsichtlich der Sehergonomie. Bei verschiedenen Sitzhaltungen soll ein	Einsatz: Berücksichtigung des Standards beim Kauf neuer Monitore Begründung: Neue Bildschirme müssen zumindest den Standard TCO '99 erfüllen.

Standard	Beschreibung/Definition	Einsatz/Begründung
	gleichmäßig gutes Sehen gewährleistet sein. Daher wurden die Bestimmungen in folgenden Bereichen verschärft: • Kontrast: 81 % (TCO '95: 64 %) • Flimmerfreiheit: >85 Hz anzustreben, mindestens jedoch 75 Hz • TCO '95 verlangt Grenzwerte hinsichtlich elektronischer Felder, elektromagnetischer Wechselfelder und Röntgenstrahlen. Die restriktiven Anforderungen werden von TCO '99 übernommen. Die Messmethoden wurden jedoch verschärft. • Verringerung der Umweltbelastung, dazu gehören: ▪ kein Einsatz von brom- und chlorhaltigen Stoffen ▪ Für alle Teile ist der Einsatz eines einheitlichen Kunststoffs zwingend vorgeschrieben. ▪ Darüber hinaus müssen die Hersteller ein Recycling nachweisen können. • Eine zentrale Forderung von TCO ist die Verminderung des Energieverbrauchs bei Computern und Monitoren. TCO '99 verlangt die Einhaltung noch restriktiverer Vorschriften: ▪ Stand-by: <15 Watt (TCO '95: <30 Watt) ▪ Automatische Abschaltung: <5 Watt (<8 Watt) ▪ Wiederherstellungszeit des Bildes: <3 Sekunden aus dem Stand-by-Modus.	
LCD-Bildschirme	LCD-Bildschirme ("Flachbildschirme") sind bei einer Gesamtbetrachtung der Wirtschaftlichkeit nicht immer teurer als vergleichbare Röhrenbildschirme, sie sind zudem platz- und stromsparend und prinzipbedingt strahlungsfrei (TCO ´99). LCD-Monitore sollten nur mit Ihrer physikalischen Auflösung betrieben werden, ansonsten wird das Bild "unscharf". Bei Fachsoftware, die für eine andere Auflösung entwickelt wurden, kann dies zu Problemen führen.	Einsatz: Unter Berücksichtigung von wirtschaftlichen, ergonomischen und arbeitsmedizinischen Gesichtspunkten ist im Einzelfall zu prüfen, welche Art von Monitor installiert wird. Flachbildschirme müssen zumindest den Standard TCO ’99 erfüllen. Der Standard "TCO ´03 Displays" wird empfohlen.
Drucker	PC-Drucker sind nach Wirtschaftlichkeitskriterien auszuwählen. Dabei ist unter Berücksichtigung von • Qualität des Drucks • Belastung des PC beim Druckvorgang • Restart des Drucks bei Abbruch oder Fehlbedienung am Drucker • Belastung durch Folgekosten insb. Kosten für Druckerfarben zu entscheiden. Um bei komplexen Sachverhalten durch Farbgebung die Verständlichkeit zu verbessern, können bei ausreichendem Bedarf Farbdrucker eingesetzt werden.	Einsatz: Bei der Beschaffung von Druckern sind die Folgekosten durch die Farbpatronen bei der Vergabeentscheidung zu berücksichtigen. Bei der Prüfung nach Wirtschaftlichkeitskriterien ist auch zu berücksichtigen, ob Multifunktionsgeräte (Drucker, Kopierer, Scanner etc. in einem) in Frage kommen
Arbeitsplatzdrucker	je nach Anforderung der Aufgabe: • Tintenstrahldrucker mit umweltschonendem Powermanagement • Laserdrucker (kleine bis mittlere Leistung) mit umweltschonendem Powermanagement	Einsatz: • Anschluss an einen oder mehreren PC (über Umschaltbox), wenn Aufgabenstellung oder Datenschutz / Datensicherheit es erfordern • Layout-Treue muss beim Ausdruck für alle Druckertypen sichergestellt werden (siehe weiter unten: PCL)
Netzwerkdrucker	leistungsfähige, ins Bürokommunikationssystem eingebundene Laser-Drucker mit umweltschonendem Powermanagement, Druckerspeicher, Anzahl Papierschächte und Papierbevorratung je nach Anforderung der Aufgabe. Unter wirtschaftlichen Aspekten können auch netzwerkfähige Multifunktionsgeräte (Kopierer / Fax / Scanner / Drucker) zum Einsatz kommen	Einsatz: • im Regelfall anstelle von mehreren Arbeitsplatzdruckern in Mehrplatz-Büros oder größeren organisatorischen Einheiten • zur Druckausgabe zentraler Batch-Auswertungen (z. B. beim Einsatz von KIFIKOS und Navision-K • bei höheren Anforderungen im Bezug auf Quantität und Qualität der Ausdrucke Layout-Treue muss für alle Druckertypen sichergestellt werden (siehe weiter unten: PCL).

Standard	Beschreibung/Definition	Einsatz/Begründung
		Begründung: • höherer Auslastungsgrad der Drucker und damit höhere Wirtschaftlichkeit • schnellere Verfügbarkeit bei Ausfall anderer Drucker
Druckersprache PCL (Hewlett Packard) Firmen-Standard	Die Druckersprache PCL (Printer Command Language) von HP ist der heutige Desktop-Standard für die Verarbeitung von Druckaufträgen im Umfeld der Bürokommunikation. Die zu druckende Seite wird vor dem Druck im Speicher des Druckers komplett aufgebaut. Die Standardisierung von PCL besagt keinesfalls, dass bevorzugt HP-Drucker beschafft werden sollen.	Einsatz: Die Versionen 5 oder 6 von PCL sind einzusetzen. Begründung: • großer Verbreitungsgrad • geringstmögliche Druck- oder Kompatibilitätsprobleme • ausgereifter Standard Bestandteil der einheitlichen IT-Infrastruktur
Elektromagnetische Verträglichkeit EMV/EMVG CE (Communauté Européenne)	Fundstelle: Normen EN 55022 und der EN 50082-1 Seit 01.01.1996 gilt für alle elektrischen und elektronischen Geräte, dass die europäischen Normen bezüglich der elektromagnetischen Verträglichkeit eingehalten werden müssen (sogenannte "Konformität"). Die europaweit gültigen Vorgaben für die EMV sind im EMV-Gesetz (EMVG) festgelegt. Mit dem Konformitätszeichen (CE) der EU wird bestätigt, dass die betreffenden elektrischen und elektronischen Geräte die gesetzlichen EMV-Richtlinien erfüllen. Seit dem 01.01.1996 ist diese CE-Konformitätsprüfung gesetzlich vorgeschrieben. Alle seit diesem Zeitpunkt hergestellten Geräte müssen das CE-Zeichen führen.	Einsatz: alle elektrischen und elektronischen Geräte in der Büroumgebung Begründung: Das CE-Zeichen wird immer verlangt. Dies ist besonders wichtig beim Einsatz von Geräten aus Asien.

2. Betriebssysteme und Systemarchitekturen

Betriebssysteme sind die Basis für alle IT-Anwendungsverfahren. Deshalb ist bei Betriebssystemen sicherzustellen, dass immer eine aktuelle und in Wartung befindliche Version zum Einsatz kommt. Nur in besonders begründeten Sonderfällen sind Ausnahmen möglich.

Als Systemarchitektur sind Client-Server-Systeme mit den definierten Clients und Servern die Regel, das Terminal-Server-System mit Terminal-Clients gibt es bei einzelnen Fachanwendungen.

2.1. Großrechner/Serverfarmen/Cluster

Standard	Beschreibung/Definition	Einsatz/Begründung
MVS	• *MVS* (*M*ultiple *V*irtual *S*ystem) Dieses Betriebssystem wurde Anfang der 70er-Jahre von IBM für die damaligen Großrechner der IBM-Systeme /370 entwickelt. Hauptmerkmal war der zu benutzende virtuelle Speicher bzw. die virtuelle Speicheradressierung. • *MVS/ESA* (*M*ultiple *V*irtual *S*torage/*E*nterprise *S*ystem *A*rchitecture) In der Version /390 neuestes Betriebssystem für IBM Großrechner. Es beinhaltet u. a.: Data-Space, Hiper-Space, ESCON, Sysplex.	Einsatz: im KRZ-SWD (vor allem für die Abwicklung des Kirchlichen Meldewesens und der Personalabrechnung)
VMS	• *VMS* Betriebssystem der VAX- und Alpha-Serie von Digital Equipment Corporation - jetzt Hewlett Packard.	Einsatz: für einzelne Fachanwendungen noch im Netz des OKR im Einsatz, die Ablösung steht unmittelbar bevor.

2.2. Server

Standard	Beschreibung/Definition	Einsatz/Begründung
Windows2000, Windows2003 de-facto-Standard	Betriebssystem von Microsoft für Server Wesentlicher Bestandteil von Windows (ab Windows 2000) sind die Active Directory Services (AD) als verteiltes Verzeichnis zur Verwaltung aller Objekte (z. B. Benutzer, Gruppen, Rechner, Dienste) innerhalb einer i. d. R. hierarchischen AD-Struktur	Einsatz: regelmäßig im Kernbereich der einheitlichen Bürokommunikation Begründung: Bestandteil der einheitlichen IT-Infrastruktur
LINUX de-facto-Standard	Linux ist ein Unix-Clone (bzw. arbeitet wie ein Unix Betriebssystem) mit 32-Bit Betriebssystem, protected-mode Unterstützung, System V kompatibel, BSD kompatibel und unterstützt den POSIX-1 Standard (Fundstelle: ISO/IEC 9945.2-1992 / IEEE Std 1003.2-1992: POSIX (Portable Operating System Interface), Part 2: Shell and Utilities). Linux wurde unter den Bestimmungen der GNU (General Public License = GPL) urheberrechtlich geschützt; d. h. es ist Teil des Open Source Initiative und es steht im Internet kostenlos zur Verfügung. Offene Punkte bei Open Source-Produkten sind: • Urheberrecht • Haftungspflicht.	Einsatz: Diese Betriebssysteme sind für Server und Clients geeignet. Im OKR-Netz werden sie im Bereich DNS, Mailrelay, PKI und Webserver eingesetzt Begründung: Anwendungsserver, Web-Server, Administrationsserver können auch mit den LINUX-Betriebssystemen betrieben werden. Der weitere, umfangreichere Einsatz ist regelmäßig zu prüfen.

2.3. Serverzentrierte Architekturen

Standard	Beschreibung/Definition	Einsatz/Begründung
Server		
MS- Terminal Services	Systemkomponente für reine Microsoft Client-Umgebung; basierend auf Windows. Die aktuelle Version ist Bestandteil von Windows 2003 Server. Die Client-Server-Kommunikation erfolgt über das Remote Desktop Protokoll (RDP).	Einsatz: Als wirtschaftliche Alternative zu Client-Server-Systemen, vor allem bei einheitlich genutzten Anwendungen, sowohl innerhalb einer Verwaltungseinheit als auch zur Konzentration der Serverdienste für mehrere Verwaltungseinheiten. Die Wirtschaftlichkeit ist im Einzelfall nachzuprüfen. Begründung: Applikationen werden immer auf dem Server ausgeführt. Nur die Interaktion mit dem Benutzer (Bildschirm, Tastatur, Maus) wird über den Client geregelt. Dadurch entstehenfolgende Vorteile: • Reduzierung der TCO • Vermeidung von PC- Ersatzbeschaffungen wegen zu geringer Leistung • bessere Performance der Anwendungen • zentrale Anwendungsadministration
Citrix Presentation Server de-facto-Standard	Server-Applikation von Citrix insbesondere für heterogene Windows-Clients, basierend auf Windows Terminal Services. Die Client-Server-Kommunikation erfolgt über das ICA-Protokoll (Independent Computing Architecture). Das ICA Protokoll ist effizienter als RDP (Remote Desktop Protocol) des MS Terminal Servers. ICA der Fa. Citrix hat die Aufgabe, die Anwendungslogik von der Benutzerschnittstelle auf dem Server zu trennen, um somit nur Tastatureingaben, Mausaktionen und Bildschirmaktualisierungen im Netzwerk vom Server zum Client zu übertragen. ICA ist ein schmalbandiges Protokoll und auch bei geringen Übertragungssgeschwindigkeiten (z. B.	Einsatz: Für Anwendungen ist im Einzelfall zu prüfen, ob für ein sog. "Serverbased Computing" MS Terminal Services allein ausreichen oder ob zusätzlich Citrix Presentation Server erforderlich ist. Begründung: MS-Terminal-Services haben gegenüber Citrix Presentation Server funktionale Defizite, die für die Administration und konkrete Anwendungen

	Modem, ISDN) geeignet.	inakzeptabel sein können.
VMware ESX-Server de-facto-Standard	VMware ESX-Server ist die virtuelle Infrastruktur-Software zur Partitionierung, Konsolidierung und Verwaltung von Systemen in geschäftskritischen Umgebungen. ESX Server und virtuelle VMware-Infrastrukturknoten bieten eine enorm skalierbare virtuelle Maschinenplattform mit erweiterten Möglichkeiten zu Ressourcen-Management, die über VMware VirtualCenter verwaltet werden kann. Die wesentlichen Vorteile sind: • Implementierung der Server-Konsolidierung • Schnellere Reaktion mit virtueller Infrastruktur • Wesentliche Verbesserung und Senkung der Kosten für Disaster Recovery-Fähigkeiten • Testszenarien mit verschiedenen Release-Ständen möglich (z. B. für Software-Entwicklung)	Einsatz: • Server-Konsolidierung • Effiziente Serverauslastung • Verbesserung und Senkung der Kosten für Desaster Recovery-Fähigkeiten • Testszenarien mit verschiedenen Release-Ständen (z. B. für Software-Entwicklung) Begründung: Ressourcenschonende Möglichkeit zur Virtualisierung von Betriebssystemumgebungen von Microsoft, Novell und Linux möglich.

3. Einheitliches Benutzerverzeichnis/Active Directory

Standard	Beschreibung/Definition	Einsatz/Begründung
MS-Active Directory Services	Die Active Directory Services stellen ein einheitliches, umfangreiches Benutzerverzeichnis dar, das standardisierte Abfrage über z. B. LDAP ermöglichen	Einsatz: globales Adressbuch, spezielle Adresslisten Begründung: Bestandteil der einheitlichen IT-Infrastruktur

V Bürokommunikation

Ein wesentlicher Anwendungsbereich für die elektronische Datenverarbeitung ist die Bürokommunikation. Dazu gehören neben der Textverarbeitung, Tabellenkalkulation, Formen des Datenaustauschs und der Kommunikation untereinander (Internet, E-Mail und FAX). Für Einzel-PCs und kleine Netzwerke sind die relevanten Programme unter Anlage 2 aufgeführt.

1. Standards der Bürokommunikation (BK)

1.1. Grundregelungen zur einheitlichen BK

Die einheitliche Bürokommunikation beinhaltet eine Festlegung von Produkten im Kernbereich.

Zur Sicherstellung einer funktionierenden Bürokommunikation muss der Einsatz entsprechender Technik erfolgen. Die getroffenen Festlegungen für einen Einsatz von Microsoft-Produkten zur Bürokommunikation bedeuten aber nicht, dass z. B. auch Anwendungsserver, deren Anwendungen als Ergänzung zur Bürokommunikation gedacht sind, nur mit Microsoft-Technik realisiert und betrieben werden dürfen. Für spezielle Anwendungen kann ggf. Open Source Software eingesetzt werden. Deshalb ist auch im Umfeld der Bürokommunikation diejenige Technik zu wählen, die funktional und wirtschaftlich die beste Lösung darstellt und die den geltenden Standards des IT-Konzepts entspricht.

1.2. Regelungen zu den Arbeitsabläufen im OKR, soweit Informationstechnologie betroffen ist

Siehe Verfügung des Vorstands vom 31. Mai 2001, geändert durch Verfügung des Vorstands vom 15. Juni 2004

2. Textverarbeitung/Dokumenten-Struktur

Die landeskirchliche Verwaltung muss einerseits alle modernen Dokumentenformate verarbeiten können und andererseits auch gewährleisten, dass die von ihr versandten Dokumente bei den wenigen Adressaten, die noch ältere Dokumentenversionen nutzen, gelesen werden können. Durch den technologischen Fortschritt und die sich abzeichnende Beachtung der Kompatibilitätsregeln durch Microsoft ist dabei inzwischen offenbar eine Qualitätsverbesserung durch den Einsatz von Word 97 bis Word 2003 möglich. Diese Kompatibilität ist beim Austausch von Dokumenten zwischen Microsoft Office und Open Office nicht in diesem Maße gegeben.

Der jetzt mögliche Umstieg auf die Office-Version 2007 von Microsoft zeichnet sich gegenüber den bisherigen Updates durch eine deutlich höhere Komplexität aus. Durch die von Microsoft konsequent anders gestaltete Bedienung der Software ergibt sich die Notwendigkeit, den Umstieg genau zu planen und ggf. einen zusätzlichen Schulungsaufwand zu berücksichtigen.

Für den Bereich des OKR-Netzes ist der Umstieg auf Office 2007 noch nicht terminiert.

Die Verwendung des Programms Acrobat ermöglicht die Erstellung von Dokumenten im Format .PDF (Portable Document Format). Diese Dokumente können mit dem frei erhältlichen Acrobat Reader in jedem Fall gelesen werden.

Standard	Beschreibung/Definition	Einsatz/Begründung
Word 97, Word 2000, Word 2002 oder Word 2003 de-facto-Standard	Dokumentenformate und Versionen des Textverarbeitungssystems MS-Word als Komponente des Office-Pakets	Einsatz: Die landeskirchliche Verwaltung setzt intern das Format Word 2000 oder Word 2002 ein. MS-Word ist Standardformat für den Dokumentenaustausch. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Word 2007	Dokumentenformate und Versionen des Textverarbeitungssystems MS-Word als Komponente des Office-Pakets, abwärtskompatibel, aber deutlich andere Handhabung erforderlich	Einsatz: Für den Bereich des OKR-Netzes ist der Umstieg auf Office 2007 noch nicht terminiert.
Acrobat (PDF aktuelle Version) Firmenstandard	PDF (Portable Document Format) ist ein Dateiformat zur Speicherung von Dokumenten. Im Format PDF gespeicherte Dokumente können sämtliche Layout- und Typografie-Informationen enthalten, die auch bei der Druckausgabe im PostScript-Format möglich sind; zusätzlich verfügt PDF über die notwendigen Leistungsmerkmale für elektronische Dokumente: Hypertext-Links, Integration von Multimedia-Elementen, Ausgabe- und Nutzungsmöglichkeiten auf allen gängigen Rechnerplattformen und Betriebssystemen, verhältnismäßig kleine Dateigröße. Das Layout eines PDF-Dokuments mit allen typografischen und grafischen Feinheiten ist unabhängig vom Ausgabemedium, d. h. ein PDF-Dokument sieht gedruckt genauso aus wie auf dem Bildschirm – unabhängig von Rechnerplattform und Browser (soweit diese die jeweilige Auflösung und Farbmöglichkeiten zulassen). Die mit dem Acrobat Writer von Adobe verfassten Dateien (PDF) können grafische, textuelle und multimediale Elemente enthalten. Mittlerweile können PDF-Dateien auch von anderen Produkten erstellt werden (z. B. Open Office).	Einsatz: Das PDF-Format soll in der elektronischen Post dort vermieden werden, wo eine Weiterverarbeitungsmöglichkeit der Dokumente gegeben sein muss. Acrobat ist zugelassen als Dokumentenformat für den Abruf von Dokumenten von Web- und Fileservern, deren Erstellungs- und Weiterverarbeitungsprozess abgeschlossen ist. In diesem Sinne ist PDF auch als zusätzliches Dokumentenformat für E-Mail-Anhänge möglich, wenn mit Open Source Software (OSS) betriebenen BK-Systemen außerhalb kommuniziert wird. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Adobe Archiv	Für die Langzeitspeicherung von Dokumenten hat die International Organization for Standardization (ISO) das Format "PDF/A" als Standard anerkannt. Die Norm ISO 19 005-1 wurde im September 2005 veröffentlicht.	
RTF de-facto-Standard	RTF (Rich Text Format) ist ein Austauschformat zwischen den unterschiedlichen Textverarbeitungssystemen. Dieses Dateiformat ist für reine Textdokumente geeignet. Entsprechende Konvertierungsprogramme sind erhältlich und werden bereits für die Erstellung von WWW-Dokumenten eingesetzt. Nachteil: In das RTF-Format konvertierte Word-Dateien können erheblich an Umfang zunehmen und an Layout-Treue verlieren.	Einsatz: zusätzliches Dokumentenformat für den Austausch von E-Mail nach vorheriger Absprache zwischen Sender und Empfänger. Begründung: Bestandteil der einheitlichen IT-Infrastruktur

3. Mail und Fax

Standard	Beschreibung/Definition	Einsatz/Begründung
Microsoft Exchange	MS Exchange unterstützt die gängigen Mail-Standards	Einsatz: im Netz des OKR Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Postfächer / Kontakte	Für alle Mitarbeiter im Evangelischen Oberkirchenrat und in den am Netzwerk angeschlossenen Dienststellen steht ein personalisiertes E-Mail-Postfach zur Verfügung. Aus Lizenzkostengründen werden für landeskirchliche Adressen keine Postfächer, sondern nur Kontakte angelegt, die auf bestehende E-Mail-Postfächer verweisen.	Einsatz: Landeskirchliche elk-wue.de Adressen.
MRS/UMS	MRS/UMS erlaubt die Computer-Telephony-Integration und die Verarbeitung unterschiedlichster Nachrichtenformat (FAX, Sprache, SMS etc.) über eine einheitliche Schnittstelle.	Im OKR-Netz wird das MRS/UMS/ CTI-System von Cycos mit der Verbindung zu MS Exchange eingesetzt.

4. Internet Formate

Standard	Beschreibung/Definition	Einsatz/Begründung
HTML W3C Standard	HTML (HyperText Markup Language) ist die Beschreibungssprache für Seiten und Dokumente im World Wide Web. Sie stellt eine Teilmenge von SGML (Standard Generalized Markup Language, ISO 8879) dar und enthält die Sprachelemente für den Entwurf von Hypertext-Dokumenten. Um die Komponenten, die Hierarchie und die Verknüpfungspunkte der Dokumente zu beschreiben, benutzt HTML diverse Tags. Während bei SGML und XML für einzelne Dokumente verschiedene DTDs verwendet werden können, setzt HTML feste DTDs ein.	Einsatz: Für den Dokumentenaustausch hat sich HTML nicht bewährt. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
XHTML	Weiterentwicklung des HTML-4-Standards. Der neue Standard für Webdesign verbessert die Logik im Dokument, macht die Seitengestaltung flexibler und erweitert HTML um fortgeschrittene XML-Techniken.	Einsatz: Dokumentenformat zur Darstellung von Webseiten. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
XML Internet-Standard	XML (Extensible Markup Language) erlaubt die systematische Definition und anwendungsübergreifende Nutzung von Dokumenten und Daten. Es ist verwandt mit der "Websprache" HTML (vor allem ab Version 4), bietet jedoch wesentlich mehr Flexibilität in der Beschreibung von Dokumenten und Daten und erleichtert so das Finden, Kategorisieren und Anpassen von Informationen im Netz. Im Gegensatz zu HTML kann XML selbst nicht direkt in einem Web-Browser angezeigt werden. Da mit XML beliebig viele Tags definiert werden können, kann deren Darstellung nicht wie bei HTML fest im Browser programmiert werden. Daher benötigt man eine besondere Stilsprache (XSL=Extensible Stylesheet Language), die XML in leichter darstellbare Formate wie HTML transformieren kann.	Einsatz: siehe Nr. 5 auch als Dokumentenformat beim Austausch über E-Mail, wobei die Einzelheiten zwischen Absender und Empfänger abzustimmen sind Begründung: Bestandteil der einheitlichen IT-Infrastruktur

5. Dokument-Vorlagen und Schrift-Typen

Standard	Beschreibung/Definition	Einsatz/Begründung
Dokumenten-Vorlagen Landeskirchlicher Standard	"Einheitliche Dokumentvorlagen" für MS Office stehen für die Benutzer im Netz des OKR in den Öffentlichen Ordnern "Allgemeine Informationen/Informationstechnologie/Word-Vorlagen" bereit.	Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Arial Landeskirchlicher Standard	True-Type Schriftartendatei zur Erstellung von Dokumenten, Tabellen etc. unter der grafischen Benutzeroberfläche Windows. Größe: 11 pt; normal Für die Schriftarten und -größen für die einheitliche Dokumentvorlage "Kopfbogen" vgl. Mitteilung der Internen Verwaltung vom 30.11.2004	Begründung: Bestandteil der einheitlichen IT-Infrastruktur

6. Organisation

6.1. Betrieb

Standard	Beschreibung/Definition	Einsatz/Begründung
Betrieb durch Eigenbetrieb Landeskirchlicher Standard	Der Betrieb der einheitlichen Bürokommunikation wird im OKR grundsätzlich nur von einer Stelle durchgeführt. Dabei können auch nur Teile z. B. über das OKR-Netz abgewickelt werden.	Einsatz: insbesondere im Kernbereich der einheitlichen Bürokommunikation innerhalb des OKR-Netzes Begründung: Bestandteil der einheitlichen IT-Infrastruktur

6.2. Fehlerbehandlung und Qualitätssteigerung in der BK

Standard	Beschreibung/Definition	Einsatz/Begründung
Fehlerbehandlung Landeskirchlicher Standard	Die Vorgehensweise, wie technische und organisatorische Fehler beim elektronischen Dokumentenaustausch behandelt und behoben werden, ist verbindlich und systematisch festgelegt. Geregelt sind hierbei insbesondere die Verantwortlichkeiten • jedes Nutzers für die Fehlermeldung • der jeweils zuständigen Mitarbeiter für die ▪ Fehlerdokumentation ▪ Fehlerklassifikation ▪ Fehlerbehebung oder Veranlassung der Fehlerbehebung ▪ Fehlereskalation Die Fehlerbehandlung erfolgt seit Einführung der Hotline innerhalb des OKR-Netzes über die Trennung zwischen First-Level-Support (=Hotline) und Second-Level-Support (Fachunterstützung) auf der Basis eines professionellen und systemgestützten Problemmanagements für die • Unterrichtung der Dienststellen • Fehlerbehebung • Rückmeldung der Fehlerbehebung	Einsatz: Insbesondere im Kernbereich der einheitlichen Bürokommunikation innerhalb des OKR-Netzes Begründung: Bestandteil der einheitlichen IT-Infrastruktur

Standard	Beschreibung/Definition	Einsatz/Begründung
Qualitätssteigerung Landeskirchlicher Standard	Die Maßnahmen werden im Referat IT, Sachgebiet EDV-Systemmanagement zusammengefasst. Spürbare Verbesserungen des Dokumentenaustausches können vor allem durch • die Einrichtung eines zentralen Systemmonitorings für die permanente Aufrechterhaltung und Optimierung der Dienste des Netzwerk-/Systembetriebs und • den Aufbau eines Problemmanagementsystems mit User-Help-Desk (HelpLine) zur organisierten und fachkompetenten Abarbeitung von Fehlern oder Anwenderfragen erreicht werden.	Einsatz: Insbesondere im Kernbereich der einheitlichen BK und beim Dokumentenaustausch innerhalb der Landeskirche

7. Festlegungen für OSS-Bürokommunikationssysteme

BK-Systeme können außerhalb des Kernbereichs der einheitlichen Bürokommunikation innerhalb des OKR-Netzes mit Open Source Software (OSS) unter Linux oder Windows betrieben werden, sofern dies insgesamt wirtschaftlich ist und hierdurch eine funktionierende Bürokommunikation mit den anderen Dienststellen innerhalb der Landeskirche und Bundes- oder Landesbehörden und dem kommunalen Bereich sichergestellt wird. Dies erfordert, dass ein Mindestumfang der oben genannten Standards erfüllt wird.

Standard	Beschreibung/Definition	Einsatz/Begründung
K Desktop Environment (KDE)	KDE erzeugt eine graphische Benutzeroberfläche, die Windows sehr ähnlich ist.	Einsatz: ist bisher nicht erprobt
OpenOffice	OpenOffice ist ein mit MS Office vergleichbares Softwarepaket für Bürofunktionen. Seine wesentlichen Komponenten sind • "Writer" für die Textverarbeitung • "Calc" für die Tabellenkalkulation • "Impress" für Präsentationsgrafiken • "Draw" für Zeichnungen • "Base" für Datenbankanwendungen. OpenOffice stellt eine Vielzahl von Filtern für den Export in Fremdformate (insbesondere die MSFormate Word und Excel) sowie den Import von Fremdformaten zur Verfügung.	Einsatz: ist bisher nicht erprobt Word-Dokumente können nur dann fehlerfrei in Open Office übernommen werden, wenn sie keine VBA-Makros enthalten. Auch führen Verbunddokumente (z. B. Word mit eingebetteten Grafiken oder Excel-Tabellen) oft zu Konvertierungsfehlern; solche Dokumente sollten im PDF- oder RTF-Format an OpenOffice-Clients versendet werden.

VI Arbeitsplatzausstattung

Hier wird der Standard-Arbeitsplatz im Evangelischen Oberkirchenrat und in direkt angeschlossenen Dienststellen beschrieben. Über die genannten Programme hinaus sind die verschiedenen Arbeitsplätze je nach Anforderung auch mit einzelnen oder mehreren zentralen Grundverfahren ausgestattet, wie sie in Kapitel VIII beschrieben sind.

Für Einzel-PCs und kleinere Dienststellen sind die Angaben zu einem Arbeitsplatz für durchschnittliche Anforderungen in der Anlage 2 zusammengestellt.

1. PC-Standard-Arbeitsplatz

Standard	Beschreibung/Definition	Einsatz/Begründung
PC-Arbeitsplatz	Für die Bürokommunikation in der Verwaltung ist der Arbeitsplatz mit folgender Standardsoftware installiert: Windows 2000 Professional: • Adobe Acrobat Reader • Adress Manager • Citrix ICA-Client • Free PDF XP • Ghostscript • IrfanView • LoginScreen • McAfee Virus Scan Enterprise • Microsoft Internet Explorer • Microsoft Office XP • Microsoft Office XP Media Content • Microsoft Remote Desktop Client • Microsoft Windows Installer 3.0 • Microsoft Windows Media Player 9.0 • O&O Defrag 2000 Freeware Edition • PowerArchiver • Real VNC 4.0 • RealPlayer • Terminalemulation VT320 • UMS Faxsoftware Windows XP Professional: • Adobe Acrobat Reader • Adress Manager • Citrix ICA-Client • Free PDF XP • Ghostscript • IrfanView • LoginScreen • McAfee Virus Scan Enterprise • Microsoft Internet Explorer • Microsoft Office XP • Microsoft Office XP Media Content • Microsoft Remote Desktop Client • Microsoft Windows Media Player 9.0 • IBM Record Now • PowerArchiver • Real VNC 4.0 • Terminalemulation VT320 • UMS Faxsoftware (Die Details dieser bis auf Konfigurationsparameter herunter reichenden Definitionen können beim Referat IT erfragt werden.)	Beispielhafte Realisierung der einheitlichen IT-Infrastruktur. Der breite Einsatz der für den PC-Arbeitsplatz getroffenen Festlegungen verhindert ein "Mehrfacherfinden" der Parametereinstellungen und erleichtert den elektronischen Dokumentenaustausch durch eine de-facto Detail-Standardisierung.

Standard	Beschreibung/Definition	Einsatz/Begründung
	Umfang von Office: Für den Standardbenutzer werden die Office-Komponenten Word, Excel und Outlook eingesetzt. Diese Applikationen sind in dem Paket OfficeXP Standard enthalten. Es ist je nach Arbeitsplatzgruppe vorgegeben, ob PowerPoint, Publisher oder Access eingesetzt werden. Zusätzliche Software: Verschiedene weitere Spezialanwendungen werden auf einzelnen Rechnern zusätzlich installiert. Vom Hersteller aufgrund von entdeckten Sicherheitslücken oder Fehlfunktionen entwickelte ServicePacks werden auf den Arbeitsplätzen aktuell gehalten	

2. Weitere Standardprogramme im Bereich Bürokommunikation

2.1. Tabellenkalkulation und Präsentationsgrafiken

Standard	Beschreibung/Definition	Einsatz/Begründung
Tabellenkalkulation MS-Excel de-facto-Standard	Softwarewerkzeug zur Tabellenkalkulation und für damit zusammenhängende Grafiken	Einsatz: generell im Rahmen der einheitlichen Bürokommunikation Exceldateien können auch nach vorheriger Absprache der jeweiligen Version per E-Mail ausgetauscht werden. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Präsentationsgrafik-programm MS-PowerPoint de-facto-Standard	Softwarewerkzeug zur Erstellung von komplexeren Grafiken, Organigrammen, Folien etc. unter der grafischen Benutzeroberfläche Windows der Fa. Microsoft	Einsatz: generell im Rahmen der einheitlichen Bürokommunikation PowerPoint-Dateien können auch nach vorheriger Absprache der jeweiligen Version per E-Mail ausgetauscht werden. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
MS-Project	Softwarewerkzeug zur Erstellung von komplexeren Projektplanungen etc. und deren Ablaufüberwachung unter der grafischen Benutzeroberfläche Windows der Fa. Microsoft	Begründung: Bestandteil der einheitlichen IT-Infrastruktur
MS-Access	Softwarewerkzeug zur Erstellung und Betrieb von kleineren Datenbankanwendungen	
MS-Publisher	Softwarewerkzeug zur Erstellung von Broschüren u. a. Publikationen	

2.2. Datenaustausch

Standard	Beschreibung/Definition	Einsatz/Begründung
XML Internet Standard	Durch die Standardisierung von XML und die Mächtigkeit der Datenvalidierung durch die Beschreibungsdatei bietet XML einen guten Standard zum Datenaustausch bis hin zur Daten-bankportierung zwischen verschiedenen Plattformen.	Einsatz: Künftig generell für Datenaustausch zwischen Datenbanken, Workflow- und Anwendungs-systemen

Standard	Beschreibung/Definition	Einsatz/Begründung
	Beispiele: • Möglichkeit für selbstbeschreibende Transaktionen • Objektbasierte Dokumenten-Daten und Regeln liegen zusammen. • Mit XML wird der Übergang vom batchorientierten Austausch zur Near-Realtime-Kommunikation möglich. • Dokumente, die mittels XML aufbereitet wurden, liegen als Klartext vor. • XML besitzt die Eigenschaft, nahezu beliebige Inhalte transportieren zu können. • Protokoll für die Replikation zwischen Datenbeständen siehe hierzu Nr. 3.5	Begründung: Kostenreduzierung beim Datenaustausch

2.3. Komprimierungsprogramme

Ein Packer ist ein Komprimierungsprogramm, mit dem mehrere Dateien zu einer einzigen Datei "zusammengepackt" werden können. Dabei nimmt die Gesamtgröße der Dateien ab. Packer werden vor allem verwendet, um Dateien, die man im Moment nicht benötigt, zu archivieren oder um große Dateien über Netzwerke mit geringer Bandbreite zu transportieren.

Standard	Beschreibung/Definition	Einsatz/Begründung
WindowsXP-Zip-Programm	Mit diesem Programm können Dateien (auch ganze Verzeichnisse) in einer Datei zusammengefasst und "stark" komprimiert werden. Damit ist es hervorragend geeignet, um Daten im Internet zur Verfügung stellen. Daten, die mit dem WindowsXP-Zip-Programm gepackt sind, erkennt man an der .zip-Endung. Um die .zip-Dateien auspacken zu können, benötigt man einen Entpacker, wozu wiederum das WindowsXP-Zip-Programm benutzt werden kann Der Aufruf von selbstextrahierenden exe-Dateien sollte nur bei aktivem lokalen Virenschutzprogramm erfolgen	Einsatz: • Verpackung von großen Dateien/Verzeichnissen, um diese z. B. mittels E-Mail kostengünstiger zu versenden • Komprimierungsformat für den E-Mail Austausch Begründung: Bestandteil der einheitlichen IT-Infrastruktur
PowerArchiver	wie oben, die Programme sind untereinander kompatibel	PowerArchiver unterstützt alle Standard-Packformate und ist sehr kostengünstig

2.4. Viewer

Standard	Beschreibung/Definition	Einsatz/Begründung
Viewer	Tool für die Visualisierung aller gängigen Dateiformate einschl. MIME-Dekodierung, Pack/Unpack und der Konvertierung in die aktuellen und älteren MS-Formate. Ein Multiformat-Viewer sollte mindestens folgende Formate unterstützen: RTF, WordPerfect, MS-Formate, Lotus-Formate, MIME, HTML, TIFF/GIF/JPEG, Zip/Unzip.	Einsatz: Viewer sind so zu installieren, dass sie mit allen MS- Applikationen verknüpft und im Posteingang und in den Ablage-Systemen aufgerufen werden können. Begründung: Bestandteil der einheitlichen IT-Infrastruktur

2.5. Workgroup-Computing

Standard	Beschreibung/Definition	Einsatz/Begründung
Workgroupprodukte Landeskirchlicher Standard	Teile: MS-Exchange MS-Outlook für E-Mail, Kalender, Termine und Aufgaben.	Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Vorgangsbearbeitung	Die Vorgangsbearbeitung erfolgt mit den Mitteln und Möglichkeiten von Windows Office, Outlook Exchange und SQL-Server oder ohne elektonische Hilfe. Im Bereich der Registratur wird Regisafe zur elektronischen Vorgangsbearbeitung eingesetzt. Hier besteht noch ein erhebliches Potenzial zum weiteren Ausbau im gesamten OKR (erste Tests in dieser Richtung laufen gegenwärtig – nähere Angaben hierzu in X.2.). Die Vorgangsbearbeitung außerhalb der Registratur erfolgt mit den Mitteln und Möglichkeiten von MS Office, Outlook Exchange und SQL-Server.	Die Einführung der ersten Stufe zur elektronischen Personalakte mit dem Produkt 'Regisafe' der Fa. Hans Held dauert noch an. Der Ausbau des elektronischen Workflows mit diesem Produkt zur weiteren Effizienzsteigerung der Prozesse des Verwaltungshandelns ist geplant.

VII Datenbanken

Größere Datenmengen können nur in Datenbanken sinnvoll erfasst, abgelegt, gesucht und gefunden werden und damit einer Verarbeitung zugeführt werden. Für das Verständnis sind hier einige Grundsätze zusammengestellt. Die Umsetzung für die einzelnen Anwendungsbereiche ergibt sich aus den anschließend beschriebenen Grundverfahren. In vielen Bereichen ist die Arbeit ohne Datenbankanwendungen heute gar nicht mehr denkbar (z. B. Finanzwesen, Meldewesen, Personalwesen, Bibliotheken…).

1. Datenbankmodelle

Standard	Beschreibung/Definition	Einsatz/Begründung
Relationales Modell mit SQL als Abfrage-, Verarbeitungs und Definitionssprache	SQL (Structured Query Language) ist die Standardsprache für relationale Datenbanken. Relationale Datenbanken arbeiten mengen- und gruppenorientiert und dienen der Speicherung von persistenten (d.h. dauerhaft gesicherten) Strukturen in normalisierter Form. SQL wurde in den siebziger Jahren von IBM für relationale Datenbanken entwickelt und 1986 von der ANSI standardisiert. SQL betrachtet Zeilen, Spalten, Felder und Schlüssel der Datenbank als Objekte. Mit dieser am meisten benutzten Datenbanksprache kann die Datenbankstruktur und die in ihr gespeicherten Daten geändert werden. Sie enthält Befehle zur Erzeugung, Modifizierung und zum Zugriff auf die in Tabellen organisierten Dateien. SQL besteht aus 4 Teilen: • Data Query Language (DQL, Datenabfrage) • Data Control Language (DCL, Rechteverwaltung) • Data Manipulation Language (DML, Datenmanipulation) • Data Definition Language (DDL, Datendefinition).	Einsatz: Datenbankanwendungen werden im Bereich der Landeskirche in der Regel zur redundanzfreien persistenten Speicherung von Daten in relationalen Datenbanken entwickelt.
Mischform SQL 3 (Objektrelational)	Die Definition von SQL 3 erweitert den bisherigen Standard um weitere Typen und um OO-Konzepte (objekt-relational). Neben Kollektionstypen sind benutzerdefinierte Datentypen (UDT), Boolean, Binary Large Objects, Character Large Objects dem bisherigen Standard hinzugefügt worden. SQL 3 erweitert SQL zu einer vollen Programmiersprache.	Einsatz: In Anwendungen, bei denen es fachlich notwendig und/oder wirtschaftlich sinnvoll ist, relational strukturierte Daten und damit verknüpfte objektstrukturierte Informationen (wie z. B. Verbunddokumente, digitale Planunterlagen) in einer gemeinsamen Datenbank persistent zu speichern und konsistent zu verwalten Begründung: • gemeinsames Datenbanksystem für relationale und objektstrukturierte Daten • Verringerung des Administrationsaufwands • Objektstrukturen bleiben weitgehend erhalten.
ODMG 3.0 Standard (inkl. OQL)	Im Rahmen des ODMG 3.0 Standards (Object Database Management Group) werden alle Bereiche definiert, die notwendig sind, um Objekt- Datenbanken, Objekt-zu-Relational-Abbildungen oder darauf basierende Produkte zu entwickeln und einzusetzen. Insbesondere wird die Abfragesprache Object Query Language (OQL, in Anlehnung an SQL) behandelt. Dabei wird auch das Binding der Programmiersprachen C++, Java und Smalltalk spezifiziert.	Einsatz: Zur persistenten Speicherung und konsistenten Verwaltung von i.d.R. komplex objektstrukturierten Informationen, die wesentliche Eigenschaften des Objektmodells wie z. B. starke oder mehrfache Vererbung nutzen oder wenn die Abbildung des objektorientierten Modells auf relationale Speicherform zu Problemen führt oder zu aufwendig wird Begründung: Die Bedeutung der objektorientierten Datenbanken wird auf Grund der starken Verbreitung der objektorientierten Anwendungsentwicklung in Zukunft erheblich zunehmen.

2. DB-Standardprodukte für Großrechner und Server

Der Einsatz anderer als der hier genannten DB-Standards bedarf der vorherigen Abstimmung mit dem Referat IT.

Standard	Beschreibung/Definition	Einsatz/Begründung
ADABAS Firmen-Standard	ADABAS ist ein Datenbankmanagementsystem der Fa. Software AG, mit dem eine hohe Anzahl an Online-Transaktionen verarbeitet und große Mengen geschäftskritischer Daten gespeichert und verwaltet werden können.	Einsatz: Alle Anwendungen auf Basis NATURAL insbesondere für MVS-Betriebssysteme (s. V.2.1)
MS-SQL Server Firmen-Standard	relationales Datenbankmanagementsystem der Fa. Microsoft. Ab Version 2000 werden auch über SQL hinausreichende OLAP-Funktionalitäten (Multidimensional Expressions MDX) unterstützt und auch für die Entwicklung komplexerer Verfahren eingesetzt werden kann. Dieses Datenbanksystem ist auf die Betriebssysteme des Herstellers Microsoft beschränkt und kann in Clustern eingesetzt werden. Beim SQL Server 2005 steht die Express-Version lizenzfrei für die Anwender zur Verfügung.	Einsatz: Insbesondere in Standard-Applikationen mit starker Ausrichtung auf die MS-Anwendungsarchitektur
MSDE Firmen-Standard	kostenfreie Datenbank-Engine der Firma Microsoft	Einsatz: • als kostengünstige Alternative für MS-SQL Server, wenn auch sonst die Wirtschaftlichkeit gegeben ist • wenn die Funktionalität und die Administrationsmöglichkeiten der MSDE ausreichen.

3. DB-Produkte aus dem Bereich Open Source

Standard	Beschreibung/Definition	Einsatz/Begründung
MySQL de-facto-Standard	Multi-User-fähiges relationales Datenbank-System, teilweise unter GNU-License veröffentlicht, welches unter UNIX/LINUX und Windows abläuft. Für den Einsatz in kommerziellen Projekten ist eine entsprechend lizenzierte Version verfügbar. MySQL ist neben Linux auch für HP-UX, Sun-Solaris im UNIX-Bereich verfügbar.	Einsatz: Der Einsatz erfolgt nur nach Abstimmung mit dem Referat IT. Auf Grund der starken Verbreitung im Internet ist ein Einsatz als DBSystem für Apache Web-Server mit LINUX interessant. Diese Lösung ist für Web-Anwendungen mit durchschnittlichem Service Level geeignet. Begründung: • kostengünstige Alternative zu DB-Standardprodukten (für bestimmte Einsatzzwecke entstehen keine Lizenzkosten.) • zunehmender Einsatz in nichtkommerziellen Projekten

4. Schnittstellen zu Datenbanken

Standard	Beschreibung/Definition	Einsatz/Begründung
ODBC de-facto-Standard	ODBC (Open Data Base Connectivity) ist • eine Architektur, die Anwendungen den gleichzeitigen Zugriff auf heterogene Datenbanksysteme ermöglicht, • eine Funktions-Schnittstelle (ODBC-API), die dem Programmierer eine einheitliche Schnittstelle zu einem DBMS bietet, • eine Spezifikation für ein Programminterface (API), welches Applikationen einen Zugriff auf verschiedene SQLDatenbanken erlaubt. Wenn eine Datenbank einen ODBC-Treiber mitliefert und die Applikation via ODBC auf die Daten zugreift, braucht der Quellcode der Applikation nicht geändert zu werden.	Begründung: Bestandteil der einheitlichen IT-Infrastruktur
OLE DB de-facto-Standard	OLE DB (Object Linking and Embedding Data Base) ist eine von Microsoft entwickelte Schnittstelle für verschiedene Datenbanken, auch solche, die SQL nicht unterstützen. Unter OLE DB können Datenbanken ausgetauscht werden, ohne den Programmcode in ASP (Active Server Pages) modifizieren zu müssen. OLE DB hat auch eine Schnittstelle zu ODBC, so dass über OLE DB auch alle Datenbanken zugänglich sind, die über ODBC zugänglich sind.	Einsatz: OLE DB ist als Standardfunktion und Schnittstelle in den MS-Office Produkten und im MS Exchange Server 2003 enthalten. Darüber hinaus ist OLE DB insbesondere zur rechnerübergreifenden Integration von Windows-Anwendungen geeignet.
JDBC de-facto-Standard	JDBC (Java Database Connectivity) Datenbankzugriffsschnittstelle für Standard-SQL; diese Programmierschnittstelle erlaubt den Zugriff von Java-basierten Systemen auf gängige Datenbanksysteme. Mit JDBC können sowohl zwei- als auch drei oder höherstufige Client-Server-Systeme aufgebaut werden (Multi-Tier-Architekturen).	Einsatz: Einsatz zur plattformunabhängigen Entwicklung von Java-Applets bzw. -Servlets für einen universellen Zugriff auf relationale Datenbanken
ADO	ADO (Active X Data Objects) ist eine von Microsoft zur Verfügung gestellte, einfach anzuwendende API für den Zugriff auf SQL-Datenbanken und andere Datenquellen. Voraussetzung ist die Verfügbarkeit eines OleDB-Providers der verwendeten Zieldatenbank. Die Kombination von ADO und OleDB ersetzt ODBC. ADO besteht aus einer Sammlung von COM-Klassen.	Einsatz: Da ODBC nicht weiterentwickelt wird, kommt ADO/OleDB bei typischen Client-Server-Anwendungen auf Windows-Clients künftig eine zentrale Bedeutung zu.

VIII Fachliche Grundverfahren

Für die Fachbereiche Finanzwesen, Meldewesen und Personalwesen werden landeskirchenweit gemeinsame Anwendungen in Rechenzentren eingesetzt. Darüber hinaus muss geprüft werden, welche Verfahren sinnvollerweise auch in Zukunft zentral angeboten werden.

1. Standards für Rechen- und Fachzentren der Landeskirche

Im Bereich der Landeskirche Württemberg sind zwei Rechenzentren (im OKR und im KRZ-SWD) eingerichtet. Im KRZ-SWD werden die sog. "Massenverfahren" für das Kirchliche Meldewesen (KIM) und die Personalabrechnungssysteme (KIDICAP, P5) abgewickelt, beim OKR die übrigen Fachanwendungen sowie die gesamte Bürokommunikation für die Verwaltungen im Oberkirchenrat und den angeschlossenen Dienststellen.

1.1. Betriebs- und Nutzungsstandards

Standard	Beschreibung/Definition	Einsatz/Begründung
Betriebskonzepte Bündelung Organisation Landeskirchlicher Standard	Die vorhandenen Betriebskonzepte beruhen auf der organisatorischen und technischen Zusammenfassung bzw. Verteilung von Aufgaben auf die beiden Rechenzentren.	

2. Grundverfahren

Nach dem IT-Konzept werden funktional vergleichbare Grundanforderungen über alle Dienststellen hinweg mit einer technisch und organisatorisch vereinheitlichten IT-Infrastruktur, die auch Anwendungssoftware einbezieht, abgedeckt.

Solche einheitlichen Strukturen werden Zug um Zug im Rahmen von Grundverfahren für Kernbereiche definiert und durch die Synode oder das Kollegium des OKR verbindlich gemacht.

Die Grundverfahren müssen nach Maßgabe der jeweils genannten Beschlüsse im jeweiligen Kernbereich eingesetzt werden. (z. B. einheitliches Verfahren 'Navision-K' im Bereich Finanzmanagement).

2.1. Finanzwesen

Standard	Beschreibung/Definition	Einsatz/Begründung
KIFIKOS	Kirchliches Finanz- und Kommunikationssystem dient der Abwicklung des kirchlichen Haushalts- und Rechnungswesens auf Grundlage der Kameralistik. Die Entwicklung erfolgte durch die KIGST eV, heutiger Support erfolgt durch die KIGST GmbH. Es handelt sich um eine ADABAS C-Datenbank, die Programme wurden in NATURAL entwickelt. Drei technische Varianten sind im Einsatz: • KIFIKOS im KRZ (im Verbund mit der Erfassungslösung KIFIKOS JuniorHP) • KIFIKOS Autonom im OKR • KIFIKOS Autonom im eigenen Netzwerk	noch bis mind. 2008 im Einsatz bei den Kirchengemeinden zur Abwicklung des Haushalts-, Kassen- und Rechnungswesens.

Standard	Beschreibung/Definition	Einsatz/Begründung
Cuzea	Computerunterstützte Erfassung für Zeitbuch in Einnahmen und Ausgaben dient der Führung des Zeitbuches auf Grundlage der Kameralistik im Offline-Vorprogramm. Es handelt sich um ein PC-Programm (Einzelplatz) auf der Basis von Microsoft Access.(Auftragsentwicklung für das Referat IT) Die Daten werden regelmäßig über die zuständigen KVSTen nach KIFIKOS übertragen, dort werden die Haushaltsplanung, die Führung des Sachbuches und der Jahresabschluss durchgeführt.	noch bis mind. 2008 im Einsatz bei nebenberuflich geführten Kirchengemeinden zur Abwicklung des Rechnungswesens Vorort-Anbindung mittels Schnittstelle an KIFIKOS.
KIFIKOS Junior HP	KIFIKOS Junior dient als Vorprogramm für KIFIKOS der Offline-Bearbeitung des kirchlichen Haushalts- und Rechnungswesens Es handelt sich um ein PC-Programm (Einzelplatz und netzwerkfähig) auf der Basis von FoxPro und Microsoft Access. Die Entwicklung erfolgte durch die KIGST eV, heutiger Support erfolgt durch die KIGST GmbH. Die in KIFIKOS Junior erfassten Daten werden regelmäßig nach KIFIKOS übertragen, dort findet die Verarbeitung statt.	noch bis mind. 2008 im Einsatz bei den Kirchengemeinden zur Abwicklung des Haushalts- und Rechnungswesens.
Microsoft BusinessSolution navision (Navision-K)	Navision-K dient der Abwicklung des kirchlichen Haushalts- und Rechnungswesens auf Grundlage der Doppik mit kameraler Oberfläche. Es handelt sich um eine ERP- Standard-Software von Microsoft Business Solutions, erweitert um zusätzliche Funktionen für das Kirchliche Finanzmanagement. Die Datenhaltung erfolgt in einer Microsoft SQL-Datenbank.	Synodalbeschluss vom 27.11.2002. Mit dem Programm Navision-K wird die KIFIKOS-Software abgelöst.
FWEXAP	Eigenentwicklung Ref. IT Finanzwesen Externe Applikationen In Vorprogrammen werden im Bereich Berechnung der Kirchensteuer-Bedarfszuweisungen und externe Zinsverteilung Bewegungsdaten erzeugt, die mittels Schnittstelle nach KIFIKOS bzw. Navision-K übertragen und dort verbucht werden.	
Cuzea-N	CuZea für Navision-K dient der Führung des Zeitbuches auf Grundlage der Kameralistik im Offline-Vorprogramm. (Weiterentwicklung von CuZea). Die Daten werden regelmäßig über die zuständigen KVSTen nach Navision-K übertragen, dort werden die Haushaltsplanung, die Führung des Sachbuches und der Jahresabschluss durchgeführt. Weitere doppische Auswertungen sind möglich.	

2.2. Meldewesen

Standard	Beschreibung/Definition	Einsatz/Begründung
Kirchliches Meldewesen Version KiGSt e.V.	Verarbeitung der gesamten Gemeindgliederdaten für den Bereich der Landeskirche im Kirchlichen Rechenzentrum Südwestdeutschland. Die Entwicklung erfolgte durch die KIGST eV. Die Verarbeitung erfolgt auf der Basis von verschiedenen Dateien, die noch nicht über eine Datenbank verbunden sind.	Das Verfahren ist in den Grundzügen seit über 30 Jahren im Einsatz und wird derzeit durch ein moderneres ersetzt (s. u.)

Standard	Beschreibung/Definition	Einsatz/Begründung
Kirchliches Meldewesen Version ECKD (KIM)	Verarbeitung der gesamten Gemeindgliederdaten für den Bereich der Landeskirche im Kirchlichen Rechenzentrum Südwestdeutschland. Die Verarbeitung erfolgt in einer ADABAS C-Datenbank, die Programme sind in NATURAL erstellt, die Bedienung erfolgt über eine web/XML-Schnittstelle.	Durch den Einsatz der Meldewesen-Software im Bereich der Landeskirchen Württemberg, Baden und Pfalz, Diözesen Rottenburg-Stuttgart und Freiburg wird eine kostengünstige gemeinsame Lösung verwendet. Mit der Anpassung des Meldewesen-Verfahrens der ECKD, KIM, auf die Verhältnisse der südwestdeutschen Landeskirchen und Diözesen wird das bisherige Verfahren abgelöst.
DaViP-W	Dient der Verarbeitung der Meldwesendaten auf der Ebene des Pfarramts bzw. des Kirchenregisteramts. Es handelt sich um ein PC-Programm (Einzelplatz und netzwerkfähig) auf der Basis von FoxPro. Die Entwicklung erfolgte im Auftrag des KRZ-SWD für die südwestdeutschen Landeskirchen und Diözesen durch eine Fremdfirma.	
AHAS	PC-Programm für die Verarbeitung der Amtshandlungsdaten auf der Ebene des Pfarramts bzw. des Kirchenregisteramts. Es handelt sich um ein PC-Programm (Einzelplatz und netzwerkfähig) auf der Basis von omnis studio. Die Entwicklung erfolgte im Auftrag des Referats IT durch eine Fremdfirma.	

2.3. Personalwesen

Standard	Beschreibung/Definition	Einsatz/Begründung
P 5 (KIDICAP)	Besoldungs- und Vergütungsabrechnung im Rechenzentrum KRZ-SWD für alle Beschäftigten der Landeskirche.	Durch den gemeinsamen Einsatz der Personalabrechungssoftware der Landeskirchen Württemberg, Baden und Pfalz, Diözesen Rottenburg-Stuttgart, Freiburg und Speyer sowie deren gesamten Diakonie und Caritas Einrichtungen wird eine kostengünstige gemeinsame Lösung verwendet.
Personal Office	Personalinformationssystem der Landeskirche u. a. für Stellenpläne, Vorbereitung der Abrechnung, Urlaubs- und Fehlzeitenverwaltung, Weiterbildungsverwaltung, Bescheinigungen, Pfarrstellenbesetzungsverfahren. Hersteller des Programms ist die Firma All for One.	Einsatz in allen Personalverwaltungen im OKR in den Kirchenbezirken und kirchlichen Werken zur Pflege der Stellenpläne. Als Vororteingabe von Personaldaten und entsprechenden Auswertemöglichkeiten lässt sich das System auch dezentral nutzen. Die Anbindung erfolgt über Internet (VPN) oder über Telefon-Wählleitung.
ETWeb-PO	Online-Pflege der Qualifikationen und Wünsche an zukünftige Pfarrstelle für Pfarrer/innen; Schnittstelle von Personal Office	Einsatz für die Strategische Personalentwicklungsplanung
Pfarrstellenkarte	Darstellung der Lage von Pfarrstellen in digitaler Karte mit Angaben zu Stellenbesetzung, sowie Markierung sich in Ausschreibung befindlicher Stellen.	Für das Personaldezernat Pfarrdienst, als Ablösung einer Landkarte mit Stecknadeln.
LDMS und Microview	Einsicht in Stammblätter, Gehaltsmitteilungsblätter, Listen der Personalabrechnung. Microview bietet dabei die Sicht auf archivierte zurückliegende Jahre. Die Programme werden über das KRZ-SWD zur Verfügung gestellt.	Einsatz v. a. für die ZGASt, jedoch auch für größere Personalverwaltungseinheiten möglich.

2.4. Weitere Anwendungen

Standard	Beschreibung/Definition	Einsatz/Begründung
Adressverwaltung combit Relationship Manager (cRM)	Verwaltung verschiedener Adressbestände der gesamten Landeskirche Hersteller: Firma combit GmbH.	Einsatz: Nutzung vor allem für Versand und Serien-drucke. Einsatz in jedem Dezernat/Referat im Ober-kirchenrat, sowie Landeskirchlichen Einrich-tungen. Zum Teil Verkettung mit anderen Programmen für die im address manager die Pflege der Adressen übernommen wird.
Kirchensteuerkappung	Eigenentwicklung Ref. IT. Bearbeitung und Abwicklung der Anträge zur Kirchensteuer-kappung, basierend auf MS SQL Server.	Einsatz: Im Fachreferat Steuern
GIDEON	Eigenentwicklung Ref. IT Gebäudeinformationssystem des Evangelischen Oberkirchen-rats auf Basis des MS SQL Server. Datenbank zur Erhebung von Informationen zu kirchenge-meindeeigenen Gebäuden (Gemeindezentren, Kirchen, Gemeindehäuser, Pfarrhäuser etc.) Erstellung einer Bauübersicht zu den Gebäuden sowie Zuordnung von Bildern und Literatur. Abwicklung der Ausgleichstock-/Energiesparfonds-/Pfarr-hausfonds-/Sonstige Instandsetzungsanträge der Kirchen-gemeinden zu Bauvorhaben an diesen Gebäuden.	Einsatz: Statistische Auswertungen zu den Gebäuden. Schneller Überblick über Vorgänge an einem Gebäude, sowie Einsichtnahme in die dazu verfassten Aktenvermerke, Bauberichte etc. Referatsübergreifender Informationsaustausch (Bauberatung – Bau- und Gemeindeaufsicht)
Liegenschaftsverwaltung	Eigenentwicklung Ref. IT Bisher als MUMPS-Anwendung auf VMS-Basis im Einsatz Die Ablösung durch ein neues Verfahren hat bereits begonnen	Einsatz: Im Bereich der Immobilienverwaltung der Landeskirche
GIMAS (neues Immobilien-Management-Programm)	Neues Verfahren für das Immobilienmanagement. Hersteller GIMAS-FIOSOFT Einführung 2007	Einsatz: Im Bereich der Immobilienverwaltung der Landeskirche
Regisafe	Dokumenten-Management und elektronische Archivierung in der öffentlichen Verwaltung Das Programm wird von der Fa. Held aus Stuttgart geliefert. Es ist in Baden Württemberg in der kommunalen Verwaltung sehr verbreitet und nimmt auch in kirchlichen Einrichtungen einen zunehmend größeren Raum ein. Die Software wird genutzt für den Aufbau und den Betrieb elektronischer Aktenbeständen (elektronischer Workflow).	Einsatz: Dient seit 2007 in der Registratur zur Erfas-sung und Recharge der Postein- und Postaus-gänge sowie als Nachweis für den Verbleib der Dokumente bei den jeweiligen Bearbeitern mit Wiedervorlagefunktion. Im Baubereich wird mit der Recherchefunktionalität gearbeitet. Außerdem ist das Programm im Bereich Kirchensteuerkappung im Einsatz. Zurzeit läuft auf dieser Basis die Einführung der ersten Stufe der elektronischen Personal-akte im Dez. 3 und 6. Begründung: Kosteneinsparungen und besserer Service im kirchlichen Verwaltungshandeln.

Standard	Beschreibung/Definition	Einsatz/Begründung
FAUST	Datenbankprogramm zur Erfassung , Verwaltung und Recherche verschiedener Archivbestände.	Einsatz: Landeskirchliches Archiv
Alephino	Bibliotheksverwaltungsprogramm zur elektronischen Erfassung, Verwaltung und Recherche der Buchbestände	Einsatz: Landeskirchliche Bibliotheken

IX Anwendungsentwicklung

Die Anwendungsentwicklung erfolgt im Referat IT durch Fachleute des jeweiligen Bereichs. Dies sind z. B. ausgebildete Programmierer mit interner oder externer Unterstützung durch IT-Spezialisten. Die eigene Anwendungsentwicklung hat heutzutage nicht mehr die Bedeutung wie früher, da zunehmend versucht wird, die gestellten Aufgaben mit Hilfe von Standardsoftware zu erledigen; ggf. muss diese angepasst werden.

Selbst in Bereichen, wo der Einsatz von Standardsoftware nicht möglich ist, wird versucht, beispielsweise über die Softwarebörse der EKD, Programme einzusetzen, die bereits an anderer Stelle für gleiche oder ähnliche Anforderungen im Einsatz sind.

Die nachfolgend aufgeführten Standards werden daher auch in den o. g. Fällen angewandt, bei denen vorhandene oder neue Standardsoftware den jeweiligen Bedürfnissen angepasst werden muss.

1. Projektmanagement

Für die Wirtschaftlichkeit des IT-Einsatzes in der Landeskirchlichen Verwaltung ist ein hochwertiges und professionelles Projektmanagement unabdingbar.

2. Vorgehensmodelle

Standard	Beschreibung/Definition	Einsatz/Begründung
Lineares Sequentielles Modell de-facto-Standard	Dieses Vorgehensmodell umfasst die aufeinander folgenden Phasen 1. Analyse 2. Design 3. Codierung 4. Test 5. Wartung Die einzelnen Phasen sind durch die Erstellung von dedizierten Dokumenten voneinander getrennt.	Einsatz: Der Einsatz sollte nur in sehr kleinen, überschaubaren Projekten erfolgen, da hier nur sehr schwerfällig auf Änderungen und Fehler reagiert werden kann. Das Modell ist nicht für Projekte mit Objektorientierung geeignet. Begründung: • sehr weit verbreitetes, seit langem praktiziertes Verfahren • leicht anwendbar • sehr einfach in Form von Gantt -Diagrammen plan- und darstellbar
RAD-Modell de-facto-Standard	RAD (Rapid Application Development) Bei diesem Prozessmodell wird das gesamte Projekt in verschiedene Module aufgeteilt, die von verschiedenen Projektteams parallel bearbeitet und dann integriert werden. Die einzelnen Teilprojekte umfassen dabei jeweils folgende Phasen : 1. Geschäftsprozess-Modellierung 2. Datenmodellierung 3. Prozessmodellierung 4. Erzeugung der Applikation 5. Test und Einsatz. Beispiel für ein modernes Prozessmodell ist der Rational Unified Process (RUP).	Einsatz: In Projekten • die sich sauber modularisieren lassen • wenn genügend Programmierer zur Verfügung stehen, um mehrere unabhängige Teams bilden zu können Begründung: Das RAD-Modell führt zu schnellen Ergebnissen. Es ist nur sinnvoll, wenn die Entwickler und die Anwender professionell mit solchen Prozessmodellen umgehen können. Es ist nicht einfach zu planen und darzustellen.

Standard	Beschreibung/Definition	Einsatz/Begründung
Inkrementelles Modell de-facto-Standard	Aufbauend auf dem linearen sequentiellen Modell werden zeitlich versetzt (um mindestens eine Phase) mehrere Teilprojekte aufgesetzt, die jedes für sich zu einem Inkrement-Produkt führen. In einem ersten Inkrement werden im Normalfall Basis-Funktionen umgesetzt, die in den folgenden Inkrements verfeinert, erweitert und perfektioniert werden. Jedes Inkrement stellt eine abgespeckte Version des angestrebten "Endproduktes" dar.	Einsatz: In Projekten, bei denen zu Anfang weniger Entwickler zur Verfügung stehen, mit der Zeit aber weitere Personen hinzugezogen werden können Begründung: Das Inkrementelle Modell bezieht die Möglichkeiten moderner Entwicklungswerkzeuge mit ein.
Wasserfallmodell de-facto-Standard	Modifiziertes, sequentielles Modell mit Rückkopplungen. Bei diesem Modell werden Probleme und erkannte Fehler in den einzelnen Phasen: 1. Anforderungsdefinition 2. System- und Softwaredesign 3. Implementierung und Modultest 4. Integration und Systemtest 5. Betrieb und Wartung in die jeweiligen vorhergehenden Phasen rückgekoppelt und eingearbeitet. Dadurch ist es möglich, die Dokumentation und den Zustand der Projekte in den einzelnen Phasen konsistent zu halten; d.h. dass Anforderungen, die erst während des Betriebs erkannt werden, in die Anforderungsdefinition eingearbeitet (Änderungsdienst) und dann durch die folgenden Schritte konsequent umgesetzt und realisiert werden.	Einsatz: Bei großen Projekten Begründung: Die Rückkopplung der einzelnen Phasen erlaubt es, neue Erkenntnisse in ein Produkt zu integrieren. Der Vorteil liegt bei einer konsequenten Umsetzung in der hohen Qualität der einzelnen Dokumente. Dieser Ansatz kann nur dann funktionieren, wenn eine effektive Versionskontrolle für das Gesamtprojekt installiert ist. Dieses Modell kommt dem normalen "Lebenszyklus" eines Programmpaketes sehr nahe, wenn permanent die Notwendigkeit besteht, sich an ändernde Umgebungsverhältnisse anzupassen.
Rational Unified Process	Der Rational Unified Process (RUP) ist ein iteratives/inkrementelles Vorgehensmodell zur Softwareentwicklung. Der RUP beruht auf "Best Practice", die den gesamten Software-Lebenszyklus abdecken: • Iterative Software-Entwicklung • Anforderungsmanagement als Grundlage des Funktionsumfangs • Komponentenbasierte Architektur • Visuelle Software-Entwicklung • Verifizierte Software-Qualität • Kontrolliertes Change Management	Einsatz: Die Anwendung des RUP kommt bei großen und komplexen Entwicklungsprojekten in Betracht. Begründung: • Industriestandard • Werkzeugunterstützt • Basisreferenz der Softwareentwicklung bei Eclipse.
V-Modell XT	Das V-Modell ist ein Vorgehensmodell zur Softwareentwicklung, das in der Bundesverwaltung den Entwicklungsstandard für IT-Systeme darstellt. Das Vorgängermodell V-Modell 97 wurde im Zuge von neuen Erkenntnissen in der Softwareentwicklung im Februar 2005 durch die Version 1.0 des V-Modell XT (XT = Extreme Tailoring) ersetzt. Hauptänderungspunkte sind hierbei • Einbindung des Auftraggebers: Bisher waren die Vorgaben auf den Auftragnehmer ausgerichtet. Nun gibt es auch Vorgehensbausteine für den Auftraggeber. • Stärkere Modularisierung: Die vier bisherigen Submodelle existieren in dieser Form nicht mehr, sondern nur noch Vorgehensbausteine, aus denen das konkrete Vorgehensmodell eines Projekts zusammengestellt wird ("tailoring"). • Stärkere Orientierung in Richtung agiler und inkrementeller Ansätze: "Weg vom Wie, hin zum Was." Das V-Modell XT gibt keinerlei Vorschriften über die zeitliche Abfolge von Vorgehensbausteinen vor. Die erzeugten Produkte stehen im Mittelpunkt.	Einsatz: Die Anwendung des V-Modells XT kommt bei großen und komplexen Entwicklungsprojekten in Betracht. Begründung: Trotz der im V-Modell XT gebotenen Möglichkeit, die Aktivitäten und Produkte an die projektspezifischen Anforderungen anzupassen, ist die Anwendung aufwendig.

Anmerkung: Von den einzelnen Modellen existieren viele Abwandlungen. Beispielsweise kann aus dem Wasserfallmodell, ergänzt um Testfälle, das sog. V-Modell erzeugt werden. Dabei werden für jede Phase des Wasserfallmodells die Abnahmekriterien für die entsprechenden Tests definiert. So werden beispielsweise mit dem Lastenheft bereits die Abnahmekriterien für den abschließenden Systemtest definiert. Durch die Rückkopplung und die Modifikationen werden solche Modelle allerdings rasch sehr komplex und damit kaum noch mit vertretbarem Aufwand plan- und steuerbar.

Die modernen Prozessmodelle lassen sich für alle Programmiermethoden (strukturierte Programmierung, objektorientiert etc.) und für alle Anwendungsgebiete (z. B. Datenbanken, BK-Applikationen) anwenden. Der wesentliche Aspekt bei der Verwendung von Prozessmodellen ist die Abgrenzung der einzelnen Phasen, die am ehesten durch die Übergabe und Erstellung von definierten Dokumenten erreicht wird (Pflichtenheft, Lastenheft, Testhandbuch, Testdokumentation, Change Historie, ...).

3. Entwicklungssysteme

Standard	Beschreibung/Definition	Einsatz/Begründung
Allgemein	Bei einem Entwicklungssystem handelt es sich um Software-Pakete, die im Wesentlichen die Projektphasen Code-Erstellung, Testen und Wartung auch mit grafischen Mitteln unterstützen. Der Funktionsumfang und die Bedienung der einzelnen Produkte und die unterstützten Plattformen und Programmiersprachen sind dabei von Hersteller zu Hersteller unterschiedlich.	Einsatz: Grafische Entwicklungssysteme entsprechen dem Stand der Technik

3.1. Entwicklungswerkzeuge einzelne Anwendungen

Standard	Beschreibung/Definition	Einsatz/Begründung
Visual Basic Firmen-Standard (Microsoft) Visual Basic for Applications (VBA) Integration von Fachanwendungen	Visual Basic ist eine Programmiersprache zur Entwicklung von Windows-Anwendungen mit grafischer Unterstützung unter grafischen Oberflächen. VBA ist ursprünglich als reine Makrosprache für das Office-Paket konzipiert worden. Bedingt durch die integrierte Entwicklungsumgebung IDE (Integrated Development Environment) ist es mit leistungsfähigen Funktionen für die Makroerstellung ausgestattet worden, die die gleichen Elemente wie die Programmiersprache Visual Basic (VB) aufweist. Auch im Funktionsumfang sind VBA V. 6.0 und VB V. 6.0 inzwischen weitgehend vereinheitlicht, so dass VBA jetzt eine Teilmenge von VB darstellt. Die Integration von Fachanwendungen in die Systemumgebung der einheitlichen BK erfolgt über VB Scripts, OLE 2, Active X und COM, bzw. DCOM.	Einsatz: Der Einsatz erfolgt überall im MS-Umfeld. Bedingt durch die steigende Verbreitung von Makroviren und deren Folgeschäden sind besondere Schutzmaßnahmen (Benutzer, Administratoren, Softwareentwickler) erforderlich. Hierzu zählen insbesondere: • lokale Einstellungen (z. B. vollständige Dateianzeige, Makroviren-Schutz für alle Office-Programme,) • Filterung durch Antiviren-Software sowohl zentral beim Exchange-Server und auch bei den Clients • Nur automatische Ausführung von signierten VB-Scripten • aktuelle Sicherheits-Patches von MS einspielen

3.2. Software-Ergonomie

Standard	Beschreibung/Definition	Einsatz/Begründung
Software-Ergonomie	Fundstelle: ISO 9241, T. 10-17 Bildschirmarbeitsplatzverordnung Die BildscharbV schreibt u. a. vor, dass i.d.R. • die Software an die auszuführende Aufgabe angepasst sein muss, • die Software entsprechend den Kenntnissen und Erfahrungen der Benutzer im Hinblick auf die auszuführende Aufgabe angepasst werden können muss,	Einsatz: Die Ergonomie-Anforderungen der Bildschirmarbeitsverordnung werden in der Landeskirche bei der Entwicklung, der Auswahl, dem Erwerb und der Änderung von Software berücksichtigt.

Standard	Beschreibung/Definition	Einsatz/Begründung
	• die Systeme den Benutzern Angaben über die jeweiligen Dialogabläufe (unmittelbar oder auf Verlangen) machen, die Beeinflussung der Dialogabläufe ermöglichen sowie evtl. Fehler bei der Handhabung beschreiben und deren Beseitigung mit begrenztem Arbeitsaufwand erlauben müssen, • ohne Wissen der Benutzer keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden darf.	
Barriere-Freiheit	Behinderte Menschen sind bei der Nutzung des Internets auf technische Hilfen angewiesen (z. B. Spezialmonitor, Lupenfunktion, Braillezeile, Sprachausgabe). Bei der Programmierung, Gestaltung und redaktioneller Pflege von solchen Internetseiten bzw. e-Government-Anwendungen müssen daher eine Vielzahl von Regeln beachtet werden. Fundstelle: Behindertengleichstellungsgesetz (BGG) vom 01.05.2002, Barrierefreie Informationstechnik-Verordnung (BITV) vom 24.07.2002 und Landesbehindertengleichstellungsgesetz (L-BGG) vom 3.5.2005 (GBl. S. 327) Technische Grundlage: Web Content Accessibility Guideline 1.0 des World Wide Web Consortiums (W3C) aus dem Jahr 1999	Einsatz: Beim Erstellen des Internetauftritts der Landeskirche wurden die Anforderungen der Barriere-Freiheit berücksichtigt.

3.3. Standardsoftware und Softwarebörse

Standard	Beschreibung/Definition	Einsatz/Begründung
Standardsoftware	Die Verantwortlichen eines IT-Projekts prüfen zunächst, ob die Aufgabenstellung des Projekts ganz oder teilweise mit Produkten der Softwarebörse gelöst werden kann. Ist dies nicht oder nur teilweise der Fall, wird im zweiten Schritt geprüft, ob am Markt eine für die ggf. vollständige Problemlösung geeignete Standardsoftware verfügbar ist. Eine Entscheidung für Eigenentwicklung oder Entwicklungsvergabe setzt diese beiden Schritte voraus.	Einsatz: Verwendung geeigneter auf dem Markt oder in der Verwaltung vorhandener Software anstelle von Neu-Entwicklung Begründung: Mit dieser Vorgehensweise können • finanzielle und personelle Ressourcen eingespart werden und • Projekte schneller in den Produktivbetrieb gehen.
zentrale Beschaffung von Software	Die EKD hat Rahmenverträge über die Beschaffung von Software mit einem Großteil der Softwarehersteller abgeschlossen. Die Beschaffung der Software kann in der Weise erfolgen, dass die Nutzer im Bereich der Landeskirche die benötigten Programme über die KIGST GmbH, Strahlenberger Str. 117 in 63067 Offenbach direkt beziehen können.	Begründung: Mit der Beschaffung über die KIGST GmbH können erhebliche Rabatte gegenüber den üblichen Verkaufspreisen in Anspruch genommen werden.
Softwarebörse EKD	Die Softwarebörse ist ein Katalog von Softwareprodukten, die • entweder in einer Landeskirche entwickelt wurden und die den anderen Landeskirchen zur Nutzung zur Verfügung gestellt werden • oder auf Grund von Lizenzverträgen oder sonstigen Bestimmungen bezogen und eingesetzt werden können.	Begründung: Vermeidung von Mehrfachentwicklungen zu gleichen Aufgabenstellungen. Das Verfahren mit der Softwarebörse bei der EKD ist bisher noch nicht geklärt. Das hängt mit der Umstrukturierung der KIGST e.V./ EKD-Koordinierungsstelle IT + Meldewesen zusammen.

X Testate und Programmfreigaben

In verschiedenen Bereichen der Landeskirche dürfen nur freigegebene Programme eingesetzt werden (s. II. Rechtliche und organisatorische Vorgaben, Richtlinien zum Einsatz der elektronischen Datenverarbeitung in der Evangelischen Landeskirche in Württemberg vom 25. März 1997 AZ 87.570 Nr. 70). Darüber hinaus sind wirtschaftliche und technische Aspekte bei Programmauswahl, Programmerstellung und Programmeinsatz zu berücksichtigen.

1. Wirtschaftlichkeitsuntersuchungen

Standard	Beschreibung/Definition	Einsatz/Begründung
IT-WiBe Verwaltungsstandard Bund	Empfehlungen und PC-Programm zur Durchführung von Wirtschaftlichkeitsberechnungen beim IT-Einsatz in der Bundesverwaltung. IT-WiBe ist auch zur Anwendung in der Landeskirche geeignet. Die aktuelle Version der ITWiBe kann vom LVN-id herunter geladen werden.	Einsatz: Als erweitertes Verfahren in größeren oder komplexen IT-Projekten. Begründung: Das Tool kann auf Grund seiner umfassenden Funktionen die Arbeit erleichtern, erfordert jedoch je nach Nutzungstiefe eine detaillierte Einarbeitung.

2. Technische und wirtschaftliche Nutzungsdauer

Standard	Beschreibung/Definition	Einsatz/Begründung
Landeskirchlicher Standard	Bei Informations-Technik (insbesondere Netzkomponenten, Hardware) wird unterschieden zwischen technischer oder wirtschaftlicher Nutzungsdauer: 1. Die technische Nutzungsdauer bezeichnet den Zeittraum, in dem ein IT-System ohne außergewöhnliche Instandsetzung oder Aufrüstung voraussichtlich genutzt werden kann. 2. Die wirtschaftliche Nutzungsdauer berücksichtigt den allgemeinen technischen Fortschritt. In der Kirchlichen Verwaltung wird diese Nutzungsdauer bestimmt durch 1. das Ergebnis der Wirtschaftlichkeitsuntersuchung und 2. die Verfügbarkeit der Haushaltsmittel.	Einsatz: Die eingesetzte Informations-Technik ist immer wieder hinsichtlich Eignung, Wirtschaftlichkeit und technologischer Fortschritte zu untersuchen.

3. Testate/Programmfreigaben

Standard	Beschreibung/Definition	Einsatz/Begründung
Landeskirchlicher Standard	Für die in § 1 der EDV-Richtlinien definierten Bereiche (Kirchliches Meldewesen, Verarbeitung sonstiger personenbezogener Daten und Kirchliches Finanzmanagement) sind entsprechende Programmfeigaben bzw. Testate die Voraussetzung für den Einsatz der Software.	Begründung: Gesetzliche Vorgaben des Datenschutzes und der Haushaltsordnung.

XI Datenschutz und Datensicherheit

Derzeit werden im Bereich des Oberkirchenrats die eingesetzten Verfahren nach dem IT-Grundschutzhandbuch des Bundesamtes für die Sicherheit in der Informationstechnik dokumentiert und die organisatorischen, infrastrukturellen und technischen IT-Sicherheitsmaßnahmen dargestellt und soweit noch nicht vorhanden, dann auch umgesetzt.

Die Erstellung und Anwendung eines IT-Sicherheitskonzepts wird allen kirchlichen Körperschaften, in denen Informationstechnologie zum Einsatz kommt, dringend empfohlen.

1. Datenschutz und -Sicherheit –Grundsatz–

Anwendungen sind nach dem Prinzip der Datensparsamkeit so zu realisieren, dass sie möglichst wenig personenbezogene Daten verarbeiten. Spezifische Datenschutz- und Sicherheitskonzepte sind, sofern noch notwendig, in Übereinstimmung mit Recht, Organisation und Technik und auf der Grundlage der Rahmenkonzepte systematisch und vollständig zu entwickeln und umzusetzen.

2. Rahmenkonzepte

Die wesentlichen Regelungen des IT-Konzepts zu Datenschutz und Datensicherheit (aufgrund der einschlägigen Vorschriften) bei Client-Server-Systemen sind:

- Freeware/Shareware aus dem Internet darf grundsätzlich dienstlich nicht eingesetzt werden. In Ausnahmefällen kann der Einsatz solcher Software aber durchaus sinnvoll sein; die dafür in Frage kommenden Programme sind in Anlage 2 -Software- zu diesem Konzept genannt.
- Der Einsatz von unzulässig beschafften oder für den Dienstgebrauch nicht freigegebenen dezentralen Systemen (Hard- und Software) ist verboten.
- Dezentrale Systeme werden nach dem Stand von Organisation und Technik (nicht nach dem Stand der Wissenschaft oder der allerneuesten Technik) gesichert.
- Jedes Computersystem wird so gesichert, dass einfache bis schutzwürdige Daten damit verarbeitet werden können. Nur für die regelmäßige Verarbeitung von als vertraulich klassifizierten Daten sind besondere Maßnahmen notwendig.
- Die Sicherheit dezentraler Systeme wird von den jeweiligen Betreibern vor der Inbetriebnahme und danach in regelmäßigen Abständen nach dem IT-Grundschutzhandbuch des BSI in einem angemessenen Detaillierungsgrad analysiert und dokumentiert. Das Ergebnis einer solchen Analyse ist letztendlich maßgeblich und bildet den Ausgangspunkt des Sicherheitskonzepts, das jede Dienststelle für ihre Client-Server-Systeme erstellt.
- Die Sicherheit eines dezentralen Systems darf nicht die Sicherheit eines anderen, mit ihm vernetzten Systems beeinflussen.
- Ein Client-Server-System wird mit dem LAN und den dort installierten Routern als Einheit gesehen und auch so gesichert.
- Im Regelbetrieb eingesetzte Sicherheitstechnik muss bewährt und erprobt sein.
- Eine Dienststelle kann ihre dezentralen Systeme im Auftrag (z. B. Outsourcing) betreiben lassen. Für Datenschutz und Datensicherheit ist in jedem Fall die Daten verarbeitende Stelle i. S. des DSG-EKD zuständig.

Verschlüsselungstechnik wird insbesondere eingesetzt, wo

- die Sensitivität oder Vertraulichkeit der Daten dies erfordert (z. B. Verschlüsselung sensibler Dokumente auf einem PC, der Zugang zum Internet hat) oder
- Schwachstellen anders nicht beseitigt werden können oder
- schutzwürdige personenbezogene Daten über Netze unbekannter Betreiber (betrifft insb. das Internet) übertragen werden oder voraussichtlich den Geltungsbereich der deutschen Gesetze verlassen oder
- durch den Einsatz der Verschlüsselungstechnik Kosten bei klassischen Sicherheitsmaßnahmen reduziert werden können (z. B. Austausch von vertraulichen Vertragsunterlagen über das Internet anstatt in Papierform).
- Die Verschlüsselungstechnik muss zu den sonstigen Sicherheitsmaßnahmen passen, dem Stand der Technik entsprechen und teure Insellösungen vermeiden. Deshalb erfolgt der Einsatz von Verschlüsselungstechnik nur im Einvernehmen mit der Stabsstelle, das so früh wie möglich herzustellen ist.
- Amerikanische Verschlüsselungstechnik kann eingesetzt werden, sofern die seit 17.07.2000 exportierbaren hoch sicheren US-Versionen eingesetzt werden.

Die technischen und organisatorischen Maßnahmen müssen auf der Basis eines vollständigen Sicherheitskonzepts systematisch eingesetzt werden, um einen insgesamt hohen Sicherheitsstandard zu erreichen.

Im Hinblick auf die organisatorischen Maßnahmen wird unterschieden zwischen Systemen, die keine personenbezogenen Daten oder nicht schutzbedürftige personenbezogene Daten verarbeiten und solchen, die schutzwürdige personenbezogene Daten verarbeiten.

Vor einer produktiven Nutzung eines dezentralen Systems wird eine Sicherheitsprüfung durchgeführt und dokumentiert. Dezentrale Systeme und jedes der dort eingesetzten IT-Verfahren zur Verarbeitung personenbezogener Daten werden nach dem vorgesehenen Freigabeverfahren durch die Landeskirche freigegeben.

3. Virenschutz und Firewalltechnik

Standard	Beschreibung/Definition	Einsatz/Begründung
Virenschutz Landes-Standard	Das durchgängige, mehrstufiges Virenschutzkonzept im IT-Konzept besteht u. a. aus: • Virenscanner beim Mailverkehr (Gateway und Postfachspeicher) HTTP/HTTPS/FTP- • permanent aktiver Virenschutz auf Server (in Echtzeit) • permanent aktiver Virenschutz auf Clients(durch Anwender nicht abschaltbar) • periodisches und automatisiertes, beim Bekannt werden neuer Viren jedoch unverzügliches Update der neuesten Anti-Viren-Pattern durch Herunterladen über das Internet und Verteilung im Netzwerk • evtl. zusätzliche Sicherheit durch den Einsatz von Anti-Viren-Produkten verschiedener Herstellern auf den einzelnen Plattformen (Exchange-Server, Clients) prüfen und ggf. realisieren.	Einsatz: Mehrstufiger Einsatz führt zu höherer Betriebssicherheit und erhöht die Datensicherheit durch Vermeidung von Datenverlusten durch bösartige Programme. Begründung: • Kosteneinsparungen durch Verhinderung von aufwendigen Wiederherstellungsmaßnahmen bei Datenverlusten/Datenzerstörung. • Bestandteil der einheitlichen IT-Infrastruktur.
Schutz gegen Makroviren	Office • Sicherheitseinstellungen in Office • Digital signierte Makros • Trust-Center für digital signierte Makros beim OKR	Einsatz: Die Kirchliche Verwaltung setzt künftig grundsätzlich nur noch digital signierte Makros ein. Für Makro-Signaturen durch den OKR gilt die in der EDV-Kommission abgestimmte Policy.

Standard	Beschreibung/Definition	Einsatz/Begründung
Standardisierter Firewall Internet-Standard	Die Aufgabe von Firewalls ist es, einen möglichst ungestörten Zugriff der Intranets der Ressorts auf das öffentliche Netzwerk zu gewährleisten, andererseits den unberechtigten Zugriff auf das eigene Netz zu verhindern. Ein Firewall stellt daher den einzigen Zugang des eigenen Netzes zum öffentlichen Netzwerk dar. Die Firewall beim OKR besteht in der Regel aus Hard- und Software-Komponenten, die entsprechend der Anforderung des IT-Konzepts ganz bestimmte Dienste freigeben. Durch die Konzentration des Zugangs auf eine einzelne Komponente werden das Sicherheits-Management und die Überwachungs- und Kontrollfunktionen wesentlich vereinfacht. Bei den Zugriffskontrollsystemen von Firewalls unterscheidet man dem Verfahren nach die Datenpaket-Filterung, das Circuit-Relay und den Application-Gateway. Alle drei Funktionalitäten setzen auf unterschiedlichen Schichten auf und verbinden das Internet mit dem Landeskirchennetz.	Einsatz: Als Protokolle, die Firewalls zu externen Netzen ohne weiteres Sicherheitskonzept mit Standard-Sicherheitsfunktionen passieren lassen, sind zugelassen: • HTTPS • SMTP • LDAP • DNS. Dies sind auch die Protokolle des standardisierten Firewalls. Die Nutzer von Firewalls müssen Restrisiken einplanen.

4. Erstellung von Sicherheitskonzepten

Standard	Beschreibung/Definition	Einsatz/Begründung
Allgemein	Fundstelle: IT-Grundschutzhandbuch des BSI, Ausgabe 2004 Bei einem Schutzbedarf "niedrig bis mittel" reichen i. d. R. die Standardsicherheitsmaßnahmen des IT-Grundschutzhandbuchs aus. Bei einem Schutzbedarf "hoch bis sehr hoch" kann es sinnvoll sein zu prüfen, ob die Standardsicherheitsmaßnahmen durch höherwertige, meist jedoch auch kostspieligere, IT-Sicherheitsmaßnahmen ergänzt oder ersetzt werden müssen. Welche zusätzlichen Maßnahmen geeignet sind, kann nach Durchführung des Basis- Sicherheitschecks nach IT-Grundschutz mittels einer ergänzenden Sicherheitsanalyse (z. B. Risikoanalyse) festgestellt werden.	Einsatz: IT-Systeme der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.
Schutzbedarfs-feststellung	Ausgehend von den 3 Grundbedrohungen 1. Verlust der Unversehrtheit 2. Verlust der Vertraulichkeit 3. Verlust der Verfügbarkeit wird für das untersuchte IT-System ermittelt, welche Schäden bzw. Folgen durch Sicherheitsverletzungen entstehen würden. Beispiele: • Verstöße gegen Gesetze, Vorschriften, Verträge • Beeinträchtigung des informationellen Selbstbestimmungsrechts • Beeinträchtigung der persönlichen Unversehrtheit • Beeinträchtigung der Aufgabenerfüllung • Finanzielle Auswirkungen. Daraus ergibt sich der konkrete Schutzbedarf.	Einsatz: IT-Anwendungen der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.
Risikoanalyse	Die Risikoanalyse setzt immer auf einer Schutzbedarfsfeststellung auf (siehe IT-Grundschutzhandbuch). Wird nach Durchführung des Basis-Sicherheitschecks nach IT-Grundschutz der Bedarf nach einer erweiterte Sicherheitsanalyse erkannt, empfiehlt es sich, zunächst eine Bedrohungsanalyse durchzuführen, bei der die bedrohten Objekte des IT-Systems und alle vorstellbaren Bedrohungen (Schwachstellenanalyse) in angemessenem Umfang ermittelt werden.	Einsatz: IT-Anwendungen der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.

Standard	Beschreibung/Definition	Einsatz/Begründung
	Die Objektbildung kann z. B. nach folgenden Gruppen gegliedert werden: 1. Infrastruktur 2. Hardware 3. Software 4. Datenträger 5. Anwendungsdaten 6. Kommunikation 7. Personen Wobei zweckmäßigerweise alle wesentlichen Prozesse und Datenströme zerlegt und die Teile auf Manipulationsmöglichkeiten hin untersucht und bewertet werden. Bei der anschließenden Risikobetrachtung werden die Schadenswerte/ Häufigkeiten der Bedrohungen für die Objekte bewertet und daraus das differenzierte Sicherheitsrisiko R (R = p*S; p= Wahrscheinlichkeit für einen Schaden, S= mittlerer Schaden) ermittelt.	
Sicherheitskonzept	Hier werden die Maßnahmen gegen die Bedrohungen ausgewählt und ihre Wirkungen beurteilt. Dabei ist zu entscheiden, welche Maßnahmen angemessen sind (Kosten-Nutzen-Betrachtung) und welches Restrisiko tragbar ist.	

5. Internet-Anschluss

Standard	Beschreibung/Definition	Einsatz/Begründung
Landeskirchlicher Standard	Netze einer Kirchlichen Verwaltung dürfen nur auf der Grundlage eines detaillierten Sicherheitskonzepts an das Internet angeschlossen werden. Benutzer des OKR-Netzes können über ein logisches Intranet mittels zentralen Internet-Zugangs des OKR, der durch ein Firewallsystem und einen zentralen Virenscanner geschützt ist, an das Internet angeschlossen werden. Die Dienststellen, die einen Internet-Zugang in ihrem LAN bereitstellen, müssen sicherstellen, dass dadurch keine Störungen, Eindringversuche oder sonstige Risiken in irgendeiner Benutzergruppe des Netzes entstehen. Bei Internet-Anschlüssen ist zudem sicherzustellen, dass durch klare Zuständigkeitsregelungen eine laufende tatsächliche Kontrolle und Aktualisierung der Technik sichergestellt ist. Datenbestände, die dem Risiko des Internetzugangs nicht ausgesetzt werden dürfen, sind durch physische Trennung oder Verschlüsselung (z. B. durch PGP) zu schützen.	Einsatz: IT-Systeme müssen so betrieben werden, dass sie andere Systeme nicht stören oder an sie Störungen weiterleiten. Durch den Betrieb eines zentralen und leistungsfähigen Internet-Anschlusses über einen mit modernen Tools professionell administrierten Firewall werden Kosten und Sicherheitsrisiken minimiert.

6. Sicherheit bei Telearbeit und bei Arbeit außerhalb der Dienststelle

Die Standards des IT-Konzepts berücksichtigen die personalrechtlichen Fragen, die Organisation der Telearbeit und Definitionen zur Telearbeit nicht, sondern beschränken sich auf Empfehlungen zu Sicherheitsmaßnahmen, die bei der Nutzung privater oder dienstlicher Geräte für dienstliche Zwecke notwendig werden. Deshalb werden die Bestimmungen in der Arbeitsrechtlichen Regelung zur Telearbeit –Dienstzimmer im Privatbereich– Beschluss der Arbeitsrechtlichen Kommission vom 8.Dezember 2006 (Abl. 62 S. 328) durch die hier genannten Sicherheitsmaßnahmen ergänzt.

Aus Sicht des IT-Konzepts kann den Bediensteten grundsätzlich erlaubt werden, mit privaten Geräten sicherheitsmäßig unbedenkliche Verarbeitungsvorgänge durchzuführen. Solche Vorgänge sind z. B. dienstliche Anrufe über private Handys, dienstlich relevante SMS über private Handys, Erstellung von Vorträgen und Vortragsfolien mit privatem PC, sofern keine sensiblen Informationen übertragen werden und durch den Datenaustausch mit dem privaten Gerät keine Gefährdung dienstlicher Informationstechnologie entsteht.

CITRIX-Portal (siehe Kapitel III Netz- und Kommunikationsstrukturen, Punkt 9. Portal, Seite 20).

Darüber hinaus gilt, dass der Nutzer privater Informationstechnologie in der Lage sein muss, die dabei anfallenden technischen Vorgänge bezüglich des Risikos zu bewerten.

Standard	Beschreibung/Definition	Einsatz/Begründung
Handys, Personal Digital Assistants, Subnotebooks und Smartphones sowie Notebooks	Sicherheitsfragen bestehen bei der genannten Gerätegruppe je nach Ausstattung und Leistungsfähigkeit der Geräte insb. bezüglich • der Vertraulichkeit bei der Verarbeitung (z. B. Vertraulichkeit von Adressverzeichnissen, Personenlisten, Vermerken z. B. im Zusammenhang mit einer Vergabe, Arbeit an öffentlichen Plätzen wie z. B. bei einer Dienstreise) • der Abschottung gegenüber Dritten (z. B. beim Vergessen eines Geräts im Zug, beim Hinterlassen eines Geräts im Hotelzimmer während der Einnahme von Mahlzeiten) • der Aktualisierung von Verzeichnissen und Dokumentenablagen (z. B. Vermeiden von falschen Verarbeitungsvorgängen) • Verhindern einer Benutzung durch Dritte (z. B. sollen Diebe eine SIM-Card oder ein Notebook nicht oder zumindest nicht ohne weiteres nutzen können) • Verhindern von zufälligen Fehlern (z. B. Bedienungsfehler).	Dienstlich bereitgestellte Geräte sind immer durch ein Passwort zu sichern. Auf einem privaten Gerät dürfen keine dienstlichen Daten verarbeitet werden. Wenn regelmäßig vertrauliche oder sensible Informationen gespeichert oder sonst verarbeitet werden und das Gerät von Dritten unbefugt benutzt werden könnte, müssen die schützenswerten Daten nach dem Stand der kommerziellen Technik verschlüsselt werden.
Telearbeitsplätze ohne direkten Zugriff auf das dienstliche Bürokommunikationssystem	Soweit kein zwingender Bedarf vorhanden ist, werden Telearbeitsplätze aus Sicherheits- und Kostengründen nur über E-Mail-Verbindungen mit dienstlichen Bürokommunikationssystemen vernetzt. Solche Telearbeitsplätze haben i. d. R außerdem Zugang zum Internet. Telearbeiter müssen beim Einsatz der Telearbeitstechnik die Wirtschaftlichkeit ständig berücksichtigen.	Wenn vertrauliche oder sensible Informationen über das Internet übertragen werden, sind die Daten bei der Übertragung zu verschlüsseln. Der Telearbeiter muss, wenn er andere Internet-Dienste als E-Mail nutzt, die Risiken kennen und sicherstellen, dass durch seine Internet-Nutzung keine Risiken für die dienstliche Informationstechnologie entstehen. Eine Authentifikation über Passwort ist vorzusehen. Die allgemein üblichen Passwort-Regelungen (vgl. z. B. Empfehlungen des Datenschutzbeauftragten im Internet) sind umzusetzen. Der Telearbeiter muss den Datenbestand auf seinem PC so verwalten, dass er alle Anforderungen der Datenschutzvorschriften (insb. Richtigkeit, Auskunft über die gespeicherten

Standard	Beschreibung/Definition	Einsatz/Begründung
		Daten und die benutzten Verfahren, Übermittlungskontrolle, Löschung z. B. bei veralteten Daten oder bei Fehldrucken) erfüllt.
Telearbeitsplätze mit direktem Zugriff auf das dienstliche Bürokommunikationssystem	Bei diesen Telearbeitsplätzen sind neben den o.g. Sicherheitsmaßnahmen noch Maßnahmen zum sicheren Zugang zu dem dienstlichen Bürokommunikationssystem zu ergreifen.	Der Zugang zum dienstlichen Bürokommunikationssystem muss zusätzlich zu den o. g. noch folgende Anforderungen erfüllen: • Sichere Authentifikation des Telearbeiters • Aktivierung der Abschottungsregeln im dienstlichen Bürokommunikationssystem beim Telearbeitszugang, die beim Zugang im Büro gelten • Verschlüsselung des Datenverkehrs, falls ausländische Netze genutzt werden könnten • Automatische Erkennung von Kommunikationsstörungen mit automatischem Abmelden des Telearbeiters. Einsatz: Im OKR wird das CITRIX-Portal (s.III.9.1) als Zugang angeboten.

7. Zugriffssicherung/Berechtigungsprüfung

Standard	Beschreibung/Definition	Einsatz/Begründung
Basis-Authentifizierung	Dieses Standard-Verfahren zur Absicherung von Benutzerzugriffen auf Serveranwendungen beruht auf der Prüfung von Benutzername und Passwort. In Intranets mit heterogenen Client-Server-Umgebungen und im Internet werden diese Login-Parameter unverschlüsselt im Netz übertragen. Daraus ergibt sich ein erhöhtes Sicherheitsrisiko. In homogenen Client-Server-Umgebungen wie z. B. Windows erfolgt diese Übertragung teilweise verschlüsselt.	Einsatz: Regelmäßig bei Grundverfahren der einheitlichen IT-Infrastruktur und bei Netzwerk- Anwendungen innerhalb des OKR-Intranets. Dieses Verfahren ist als Sicherheitsmaßnahme im Internet grundsätzlich nicht geeignet.
Höherwertige Authentifizierung Internet-Standard	Dieses Verfahren unterstützt sowohl die Authentifizierung als auch die gesicherte Datenübertragung. Für eine sichere und vertrauliche Kommunikation über öffentliche Netze sind folgende Lösungen einzusetzen: • Kommunikationsebene: Basis SSL V.3 bzw. TLS V1.0 ggf. mit Client-Authentifizierung ; SSL/TLS nutzt die Public Key Kryptografie zur Authentifizierung und die Secret Key Kryptografie zur Verschlüsselung der auszutauschenden Nachrichten; die Schlüsselzertifikate (Client und Server) müssen von Zertifizierungsinstanzen stammen, die von Clients und Server anerkannt werden. • Anwendungsebene: Einmalpasswörter in Verbindung mit Authentifizierungsservern ermöglichen ein sicheres Login. Einmalpasswörter werden für jeden Loginvorgang auf speziell programmierten Token neu erzeugt. Für den sicheren Datenaustausch sorgen dann Verschlüsselungsprogramme.	Einsatz: Insbesondere wenn Zugriffe über fremde Netze erfolgen oder wenn ein Firewall einfacher gestaltet werden soll, ist eine Sicherung über die SSL-Mechanismen geboten.

8. Kryptografische Verfahren

8.1. Kryptografische Standards

Schlüssellänge und Verfahren sind bei den kryptografischen Standards zusammenhängend zu betrachten.

Standard	Beschreibung/Definition	Einsatz/Begründung
Symmetrische Verfahren		Einsatz: Typisches Anwendungsgebiet für symmetrische Algorithmen ist die vertrauliche Speicherung von Daten auf lokalen Laufwerken (z. B. Festplatten, Disketten) oder auf einem Server
DES ANSI-Standard	Fundstelle: ANSI (American National Standards Institute) X3.92-1981 (Data Encryption Standard) Der DES-Algorithmus (für Anwendungs- und Kommunikationsebene) ist ein Blockchiffrierer, der unter Verwendung eines 64 Bit Schlüssels (56 Bits signifikant, 8 Paritätsbits) 64 Bits Klartext in 64 Bits Schlüsseltext transformiert	Einsatz: Vom Einsatz wird abgeraten Begründung: DES ist zwar weit verbreitet, allerdings auf Grund der geringen Schlüsselgröße von 56 Bits umstritten.
3DES NIST-Standard	Fundstelle: NIST -Standard (National Institute of Standards and Technology) Triple-DES (3DES) erhöht die Sicherheit des normalen DES-Verfahrens, indem die Daten mit doppelter (112 Bit) oder dreifacher (168 Bit) Schlüssellänge verschlüsselt werden.	Einsatz: Stärkere Verschlüsselung, deshalb Einsatz bei höherem Sicherheitsbedarf sinnvoll.
IDEA	IDEA (International Data Encryption Standard) ist ähnlich wie DES ein symmetrischer IDEA (International Data Encryption Standard) ist ähnlich wie DES ein symmetrischer Verschlüsselungs-Algorithmus. IDEA verwendet eine Schlüssellänge von 128 Bit.	Wie 3DES
AES	AES (Advanced Encryption Standard, auch Rijndael genannt) soll den DES Standard ablösen. Das National Institute of Standards and Technology (NIST) hat AES am 26.11.2001 zum Standard erklärt. Erste Produkte sind verfügbar. Geforderte Schlüssellängen im AES-Standard sind 128, 192 und 256 Bit.	Einsatz: Da inzwischen in der Presse erste Berichte zu erfolgreichen Angriffen auf AES erschienen sind, sollten vor einem Einsatz noch weitere Erfahrungen abgewartet werden.
Asymmetrische Verfahren		
RSA	Fundstelle: R. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM*, Jahrgang 21, Nr. 2 (1978) RSA basiert auf dem Schlüsselaustausch-Algorithmus von Diffie-Hellmann (1976), der die Grundlage für die Public Key Kryptografie darstellt. Während symmetrische Verfahren darauf beruhen, dass Daten und Informationen mit demselben Schlüssel ver- und entschlüsselt werden, wird beim asymmetrischen Verfahren ein Schlüsselpaar, bestehend aus dem geheimen (private Key) und dem öffentlichen Schlüssel (public Key) verwendet. Daten, die mit einem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem zugehörigen geheimen Schlüssel entschlüsselt werden und umgekehrt. Die Berechnung des geheimen Schlüssels zu einem vorgegebenen öffentlichen Schlüssel beruht beim RSA-Verfahren auf der Faktorisierung großer Zahlen, d.h. der Zerlegung in ihre Primfaktoren. Das RSA-Verfahren ist auch die Grundlage für die elektronische Signatur, bei der die zu signierenden Daten zunächst mit einem geeigneten Zufallsverfahren komprimiert werden	Einsatz: Regelmäßig im Zusammenhang mit allen Verfahren zur • Ende-zu-Ende- Verschlüsselung der elektronischen Post • elektronischen Signatur Begründung: RSA ist heute Standard für die asymmetrische Verschlüsselung mit und ohne Chipkarten bis Schlüssellangen von ca. 2048 Bits. Für größere Schlüssellängen wird das Verfahren bei der elektronischen Signatur und Entschlüsselung sehr aufwendig. Deshalb ist hier die Elliptic Curve Cryptography (ECC) als Alternative zu RSA sehr stark im Kommen.

Standard	Beschreibung/Definition	Einsatz/Begründung
	und dieses Komprimat dann mit dem geheimen Schlüssel des Signierenden verschlüsselt werden. In Verbindung mit einer durch ein Zertifikat erfolgten Personalisierung des zugehörigen öffentlichen Schlüssels kann der Nachweis der Unversehrtheit der signierten Daten und der Authentizität des Signierenden erbracht werden.	
DSS	Fundstelle: NIST FIPS Publication 186: *Digital Signature Standard*, Mai 1994: 1984 hat El'gamal einen zu RSA alternativen Signaturalgorithmus vorgeschlagen. Eine Variante dieses El'gamal-Verfahrens ist der 1991 von NIST publizierte Standard DSS, der den Digital Signature Algorithmus (DSA) spezifiziert. Neue Varianten des DSA basieren auf Punktegruppen elliptischer Kurven.	Einsatz: Ggf. künftig als Alternative zu RSA für die elektronische Signatur zulässig Begründung: Veröffentlichung der RegTP über "Geeignete Kryptoalgorithmen", BundesAnz. Nr. 158 S. 18 562 vom 24.08.2001
Hybrid Verfahren	Kombination aus symmetrischen (in der Regel DES, 3DES) und asymmetrischen Verfahren (RSA) (siehe S/MIME und PGP, Nr. 9.6.2) Hierbei wird die Nachricht vom Absender zunächst mit einem zufällig generierten Schlüssel symmetrisch verschlüsselt. Der verwendete Schlüssel wird dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und zusammen mit der symmetrisch verschlüsselten Nachricht übermittelt.	Einsatz: Regelmäßig bei allen Verfahren zur Ende-zu-Ende-Verschlüsselung der elektronischen Post.

8.2. Verschlüsselungs-Software

Standard	Beschreibung/Definition	Einsatz/Begründung
Verschlüsselung auf Kommunikationsebene		
SSL V. 3 IETF-Standard TLS V1.0	SSL ist eine Entwicklung von Netscape für die sichere Datenkommunikation im WWW, kann jedoch auch für andere Anwendungsprotokolle der TCP/IP-Familie wie Telnet, FTP eingesetzt werden. SSL wird von allen gängigen Internet-Browsern und Server-Produkten unterstützt. Die Spezifikation zu SSL wurde Ende 1995 der Internet Engineering Task Force (IETF) zur Standardisierung vorgelegt. Aktuell ist die Version 3.2 von November 1996, die als Internet-Draft vorliegt. TLS (Transport Layer Security) ist eine Weiterentwicklung von SSL V.3. Die Protokoll-Version 1.0 wurde 1999 veröffentlicht (RFC 2246). Im Gegensatz zu SSL V.3 ist bei TLS V1.0 die Server-Authentifikation optional. Zur Vermeidung von sog. "man-in-the-middle"-Attacken sollte auf diese Funktion jedoch nicht verzichtet werden.	Einsatz: • für die Sicherung besonderer Inhalte im Netz des OKR. Im Intranetverbund ist die sichere US-Exportversion ausreichend. Das Root-Zertifikat (=Zertifizierungsstellen-Zertifikat) wird bereitgestellt Begründung: Bestandteil der einheitlichen IT-Infrastruktur
IPSec IETF-Standard	Bezeichnung für einen Standard, der Verschlüsselung und Authentifizierung für IP-Netze auf der Vermittlungsschicht regelt IPSec ist sowohl für IPv4 als auch für IPv6 definiert. Die Sicherheit gewährleistet IPSec über einen Authentifizierungsheader und ein Sicherheitseinkapselungspaket (Encapsulating Security Payload -ESP-). Im ESP sind die Nutzdaten des Paketes oder ein komplettes Paket (Tunneling) mit einem symmetrischen Algorithmus (DES, 3DES oder IDES) verschlüsselt. IPSec steht in den heutigen Routern z. B. von CISCO und in Verschlüsselungsboxen z. B. von Utimaco, Biodata zur Verfügung. Innerhalb des FreeS/WAN Projektes gibt es zwei frei verfügbare und durch Exportrestriktionen nicht reglementierte	Einsatz: für die Realisierung von VPN-Lösungen und Tunneling z. B. • zur besonderen Sicherung von Benutzergruppen (z. B. PersonalOffice-Anwender) oder • anstelle von Verschlüsselungslösungen auf Anwendungsebene (z. B. SSL)

Standard	Beschreibung/Definition	Einsatz/Begründung
	Versionen von IPSec für Linux: • Pluto • JI's IPSec von John Ioannidis.	
IKE IETF-Standard	IKE ist ein von der Firma Cisco und der IETF erarbeiteter Protokollrahmen zur Verwaltung von Security Associations in IPSec. ISAKMP (Internet Security Association Key Management Protocol) ist nur ein Rahmenwerk. Eine konkrete Umsetzung ist IKE. Internet Key Exchange (IKE) ist ein Protokoll, das der Verwaltung von Sicherheitskomponenten innerhalb von mit IPSec realisierten VPN dient. IKE wird benötigt, da IPSec die zur Verschlüsselung notwendigen Informationen (Algorithmus, Schlüssel, Gültigkeitsdauer etc.) nicht selbst überträgt, sondern sie aus einer lokalen Sicherheits-Datenbank übernimmt.	Einsatz: Der Einsatz ist in VPN Lösungen zum Austausch von Sicherheitsinformationen erforderlich.
Verschlüsselung auf Anwendungsebene		
Pretty Good Privacy de-facto- Standard	PGP (Pretty Good Privacy), Hybridverfahren aus RSA und IDEA, also eine Kombination aus symmetrischen mit asymmetrischen Verfahren, Public-Key-Verfahren zur Verschlüsselung von Daten PGP ist bei privater Nutzung lizenzkostenfrei; die Nutzung innerhalb der Verwaltung ist jedoch lizenzpflichtig. Für PGP gibt es Plug-Ins sowohl für MS-Outlook als auch für die Mail-Clients der Standard-Web-Browser (MS Outlook-Express, Netscape Messenger). Internet Freeware/ Shareware kann dienstlich nicht eingesetzt werden (vgl. Nr. 9.2). Alternativ kann das vom BSI geförderte GNU Privacy Guard (GnuPG) eingesetzt werden. Allerdings sind GnuPG und PGP derzeit noch nicht vollständig miteinander interoperabel.	Einsatz: soweit zweckmäßig zur • Ende-zu-Ende-Verschlüs-selung der elektronischen Post mit Externen, soweit nicht die gesetzeskonforme elektronische Signatur anzuwenden ist • zum Schutz bei Internetanschlüssen für die Verschlüsselung von lokal zu speichernden Dateien Begründung: Bestandteil der einheitlichen IT-Infrastruktur
MailTrusT (MTT) Nationaler Standard	Standard des Industrieverbands Teletrust e.V., dem alle wichtigen deutschen Hersteller kryptografischer Softwareprodukte für die Ende-zu- Ende-Verschlüsselung angehören MTT setzt auf dem Standard PEM (Privacy Enhanced Mail) auf. Die Version 2 ist weitgehend mit S/MIME V3 identisch und enthält unter anderem: • S/MIME als Austauschformat • Zertifikatsformate nach X.509 V. 3. Der Einsatz mit Mail-Clients von Web- Browsern (z. B. Outlook Express, Netscape Messenger) ist derzeit nur beschränkt möglich. Die Interoperabilität der Produkte auf der Basis von MTT V.2 wurde im Rahmen des Sphinx-Projektes des Bundes untersucht. Um Interoperabilität zwischen unterschiedlichen PKI-Lösungen für die Verschlüsselung (nach MTT V. 2) und die - insbesondere qualifizierte - elektronische Signatur (entsprechend den "Industrial Signature Interoperability Specifications" [ISIS V. 1.2], einem von der Arbeitsgemeinschaft der deutschen Trust Center [AGTC] verabschiedeten Standard) zu erzielen, wurde mit ISIS-MTT ein gemeinsamer Standard entwickelt, der als Version 1.02 seit 19.07.2002 vorliegt. Trust Center bieten inzwischen spezielle Dienstleistungen nach dem ISIS-MTTStandard an (z. B. Zeitstempeldienst der Fa. TTeleSec). Nach den Erfahrungen von Fa. Datev und Fa. secaron unterstützen die auf dem Markt verfügbaren Microsoft-Anwendungen Zertifikate gemäß ISIS-MTT-Spezifikation.	Einsatz: In der landeskirchlichen Verwaltung können im Rahmen dereinheitlichen Bürokommunikation solche Produkte für die Ende-zu-Ende-Verschlüsselung der elektronischen Post eingesetzt werden, die dem Mail-TrusT-Standard V. 2 und ISIS-MTT V 1.02 entsprechen. Danach ist diese Verschlüsselungstechnik in der Regel • nicht einzusetzen beim Versand im LAN • einzusetzen beim Versand über das Internet oder andere unbekannte Netze, sofern im Einzelfall z. B. auf Grund der geringen Schutzbedürftigkeit der versendeten Daten nicht anders entschieden wird. Begründung: Bestandteil der einheitlichen IT-Infrastruktur. ISISMTT wird zu gegebener Zeit aufgenommen.
S/MIME Firmen-Standard	S/MIME basiert ebenfalls auf dem asymmetrischen Schlüsselsystem. Im direkten Vergleich zu PGP ergeben sich folgende Unterschiede: • Im Gegensatz zu PGP bedarf S/MIME immer des Einsatzes von Schlüsselzertfikaten, die von einem Trust Center ausge-	Einsatz: Für die Verschlüsselung von E-Mails ist S/MIME mit einem starken Verschlüsselungsalgorithmus (mindestens 112 Bits Schüssellänge) einzusetzen.

Standard	Beschreibung/Definition	Einsatz/Begründung
	stellt werden. • Weiterhin wird, im Unterschied zu PGP, bei der elektronischen Signatur einer E-Mail immer zwingend das Zertifikat des öffentlichen Schlüssels entsprechend X 509 V. 3 angehängt. • S/MIME garantiert durch die Mail-Struktur nach PKCS # 7, dass eine an mehrere Empfänger (z. B. Verteilerliste) gerichtete verschlüsselte Mail für alle Empfänger dasselbe Format besitzt.	(vgl. Regelungen zu MTT) Begründung: Bestandteil der einheitlichen IT-Infrastruktur

8.3. Standard für Schlüssel-Zertifikate

Standard	Beschreibung/Definition	Einsatz/Begründung
X.509 ITU-Standard	Fundstelle: X.509 ist ursprünglich ein IEEE-Standard, der von der ITU übernommen wurde. Der gebräuchliche Standard für digitale Zertifikate ist der ITU Standard X.509v3. X.509 setzt auf den Namenskonventionen des Verzeichnis-Standards X.500 auf. X.509 definiert den Aufbau und Inhalt (Attribute) für die Zertifikate öffentlicher Schlüssel im Rahmen einer so genannten PKI (Public Key Infrastructure). Ein solches Zertifikat enthält neben dem öffentlichen Schlüssel des Eigentümers Angaben zur Identifikation (Name, ggf. Wohnort, etc.) des Eigentümers und zum Zertifikat selbst (Name der Zertifizierungsstelle, Gültigkeitsdauer des Zertifikats, X.509-Version, Zertifikats-Nummer, etc). Darüber hinaus enthalten Zertifikate i.d.R. eine elektronische Signatur der Zertifizierungsstelle. X.509v3 unterscheidet sich von seinen Vorgänger- Versionen insbesondere dadurch, dass weitere Angaben zum Eigentümer (z. B. Geburtsdatum) oder zum Zertifikat als sog. Extensions hinzugefügt werden können.	Einsatz: Regelmäßig beim Einsatz von asymmetrischen oder hybriden Verschlüsselungsverfahren und bei der elektronischen Signatur. Begründung: Wird eine Institution oder Person zertifiziert, so geschieht dies über die eindeutige Bindung ihres öffentlichen Schlüssels an ihren Namen und weitere Attributinformationen, die das zu zertifizierende Subjekt charakterisieren. Eine Zertifizierungsstelle bestätigt als vertrauenswürdiger Dritter diese Bindung mit elektronischer Signatur. Im Netz des OKR werden die Zertifikate in ein Einheitliches Benutzerverzeichnis eingestellt und können von dort z. B. per LDAP oder http abgerufen werden.

8.4. PKI-Konzept

Um die rechtlichen Anforderungen der Datenschlüsselungsverordnung umzusetzen wurde im Evangelischen Oberkirchenrat eine PKI (Public Key Infrastructure) auf Basis von S/MIME aufgebaut.

Für das Ausstellen und Verteilen der Zertifikate steht im Evangelischen Oberkirchenrat ein Server als Zertifizierungsstelle zur Verfügung. Hier können Zertifikate angefordert und abgeholt werden. Die Zertifikate werden dann auf dem lokalen Rechner gespeichert und stehen damit zur Verfügung. Auch die öffentlichen Schlüssel evtl. E-Mail-Partner können von diesem Server abgeholt werden.

Der Zugang zum Zertifikatsserver erfolgt über die Internet-Adresse: http://pki.elk-wue.de.

Standard	Beschreibung/Definition	Einsatz/Begründung
PKI für die E-Mail-Verschlüsselung	Für eine verschlüsselte Übertragung benötigen Sender und Empfänger ein digitales Zertifikat. Ein digitales Zertifikat ist ein Datensatz, der Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, die E-Mail Adresse, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle enthält. Eine digitale Signatur schützt diesen Datensatz gegen Veränderung. Jeder Teilnehmer an der Verschlüsselung hat einen "Öffentlichen Schlüssel", den jeder bei einer im Netz zugänglichen Stelle abholen kann und der nur zur Verschlüsselung an ihn gerichteter Nachrichten dient. Der Absender verschlüsselt E-Mails mit dem öffentlichen Schlüssel des Empfängers und versendet sie. Nur der Empfänger kann verschlüsselte E-Mail mit seinem privaten Schlüssel entschlüsseln und damit lesen.	Einsatz: Um den dienstlichen E-Mail-Verkehr zwischen Oberkirchenrat, den Kirchlichen Verwaltungsstellen, den Prälaturen, Dekanatämtern und Pfarrämtern in verschlüsselter Form abwickeln zu können, wurde im Evangelischen Oberkirchenrat die Infrastruktur auf der Basis des S/MIME Standards (Secure / Multipurpose Internet Mail Extension, Sicherheits-Erweiterung der E-Mail-Kommunikation) eingerichtet. Für den verschlüsselten Datenverkehr zwischen weiteren Datenstellen kann auch PGP (Pretty Good Privacy, bekannte Verschlüsselungssoftware für Einzelrechner) eingesetzt werden.

Anlagen

Anlage 1: Hardware und Systeme für externe Dienststellen

Diese Anlage enthält Empfehlungen zur Hardware- und zur Netz-Konzeption für kleine und mittlere Einrichtungen (in Ergänzung zum IT-Konzept). Sie wurde erstellt unter Berücksichtigung der im IT-Konzept ausführlich beschriebenen Standards, beschränkt sich aber in den Ratschlägen für die Umsetzung auf die für kleinere und mittlere Dienststellen in erster Linie wichtigen praktischen Erfahrungen.

Für die Umsetzung wurde von drei Kategorien ausgegangen:

1. Dienststellen mit Einzel-PCs
2. Dienststellen mit Vernetzung und bis zu 5 PCs
3. Dienststellen mit Vernetzung und über 5 PCs

Anmerkung: Windows Vista und Office 2007 sind neue Softwareprodukte der Firma Microsoft. Gegenwärtig unterstützt Windows Vista noch nicht alle Anwendungsprogramme unserer Landeskirche (z. B. Kifikos). Insbesondere im Modul PowerPoint und im Makrobereich sollte zurzeit. mit Kompatibilitätsproblemen gerechnet werden, die sich durch spezielle Tools von MS nicht vollständig beseitigen lassen. Aus diesen Gründen wird gegenwärtig nicht empfohlen, Windows Vista und Office 2007 umgehend einzusetzen. Es wird an dieser Stelle ausdrücklich darauf hingewiesen, dass es sich hierbei um eine vorläufige Empfehlung handelt.

1. Dienststellen mit 1-2 Einzel-PCs:

Gerät/Ausstattung:	Bemerkung:
PC mit: • Prozessor Intel/AMD mit ca. 3GHz bzw. Dual Core Prozessoren • Hauptspeicher: 512 - 1024 MB • Festplatte: 80 – 250 GB • CD/DVD-Brenner • Microsoft Windows XP Professional • Microsoft Office XP oder 2003	Für die normale Bürotätigkeit reicht ein PC im mittleren Preissegment aus. Höhere Rechenleistung ist nur notwendig wenn häufig aufwendige Bildbearbeitung gemacht werden soll. Höchste Rechenleistung ist meist überproportional teuer. Für die Datensicherung bietet sich je nach Menge der Daten ein DVD oder CD-Brenner an, da diese eine einfache Handhabung sowohl bei Sicherung als auch bei der Wiederherstellung der Daten bieten. Als Betriebssystem sollte MS Windows XP Professional eingesetzt werden, da dieses stabil läuft und auch relativ viele Programme dafür verfügbar sind. Außerdem unterstützt der OKR momentan nur MS Win XP Professional (oder ältere MS Betriebssysteme) für seine Programme. Im Gegensatz zur Home-Variante ermöglicht Professional differenziertere Sicherheitseinstellungen und ermöglicht später auch eine professionelle Vernetzung. Für die Bürokommunikation empfiehlt es sich MS Office XP oder 2003 zu nehmen, da dies einen problemlosen Austausch von Dokumenten mit vielen anderen Dienststellen ermöglicht – MS-Office ist derzeit Defacto Standard.
Internet-Zugang • ISDN-Karte: z. B. AVM Fritz!Card (für Internetanbindung); • Netzwerkkarte und DSL-Modem für DSL-Internetzugang	Für den Internetzugang stehen als Alternativen ISDN oder DSL zur Verfügung. ISDN ist zu empfehlen wenn nur gelegentlich Informationen aus dem Internet abgerufen werden. DSL rentiert sich bei Online-Zeiten von mehr als ca. 40 Std./Monat oder großen Download-Mengen, da hierfür sog. Flatrates verfügbar sind.
Funk-LAN	Funk-LANs bzw. Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen Aufgrund der bequemen Einrichtung der WLAN-Netze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA Verschlüsselung einschalten (langes Kennwort)

Gerät/Ausstattung:	Bemerkung:
	• Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren, werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
E-Mail	Für E-Mail-Kommunikation stehen derzeit mehrere Programme zur Verfügung. Outlook Express ist kostenlos im Betriebssystem enthalten, während Outlook meist mit dem Office-Paket geliefert wird. Alternativ gibt es noch Mozilla Thunderbird.
Virenschutz + Personal-Firewall	Unbedingt notwendig ist ein Virenschutz der regelmäßig (am besten automatisch) aktualisiert wird. Alternativ zur Firewall von Windows kann eine Personal-Firewall verwendet werden, die differenzierte Einstellungen ermöglicht.
Drucker: Tintenstrahldrucker; alternativ Laserdrucker	Welche Druckerart man wählt hängt von der Art und der Menge der zu druckenden Dokumente ab. Tintenstrahldrucker sind in der Anschaffung günstig und bieten die Möglichkeit, farbige Ausdrucke zu machen. Allerdings sind die Druckkosten pro Seite relativ teuer, speziell bei Farbdrucken. Sie eignen sich somit für gelegentliche Ausdrucke mit farbigen Elementen. Laserdrucker bieten erst bei teureren Modellen Farbdrucke. Die kleineren Monochrom-Modelle eigenen sich vor allem für kleine bis mittlere Druckvolumina, die keinen Farbdruck erfordern. Die Kosten pro Seite sind deutlich geringer als bei Tintenstrahldruckern.
Scanner	In der Regel sind die meisten Modelle für den Bürogebrauch geeignet. Sollen aber gelegentlich Dias gescannt werden, muss ein Modell gewählt werden, das eine sog. Durchlichteinheit hat.
Zugang zum OKR-Netz: Zugangskennungen	Auf den Rechnern des OKR werden neben der Bürokommunikation eine Reihe weiterer Anwendungen im Bereich Personalwesen, Finanzwesen u. a. angeboten. Der Zugang erfolgt üblicherweise über das Internet und das Produkt Citrix, das auf dem lokalen PC installiert wird. Die Zugangskennung vergibt das Referat IT.

2. Dienststellen mit bis ca. 5 PCs:

Gerät:	Bemerkung:
PC(s) mit: • Prozessor Intel/AMD mit ca. 3GHz bzw. Dual Core Prozessoren • Hauptspeicher: 512 - 1024MB • Festplatte: 80 – 250 GB • CD/DVD-Brenner • Netzwerkkarte für Peer-to-Peer-Vernetzung • Microsoft Windows XP Professional • Microsoft Office XP oder 2003	Für die normale Bürotätigkeit reicht ein PC im mittleren Preissegment aus. Höhere Rechenleistung ist nur notwendig wenn häufig aufwendige Bildbearbeitung gemacht werden soll. Höchste Rechenleistung ist meist überproportional teuer. Für die Datensicherung bietet sich je nach Menge der Daten ein DVD oder CD-Brenner an, da diese eine einfache Handhabung sowohl bei Sicherung als auch bei der Wiederherstellung der Daten bieten. Als Betriebssystem sollte MS Windows XP Professional eingesetzt werden, da dieses stabil läuft und auch relativ viele Programme dafür verfügbar sind. Außerdem unterstützt der OKR momentan nur MS Win XP Professional (oder ältere MS Betriebssysteme) für seine Programme. Im Gegensatz zur Home-Variante ermöglicht Professional differenziertere Sicherheitseinstellungen und ermöglicht später auch eine professionelle Vernetzung. Für die Bürokommunikation empfiehlt es sich MS Office XP oder 2003 zu nehmen, da dies einen problemlosen Austausch von Dokumenten mit vielen anderen Dienststellen ermöglicht – MS-Office ist derzeit Defacto Standard.
E-Mail	Für E-Mail-Kommunikation stehen derzeit mehrere Programme zur Verfügung. Outlook Express ist kostenlos im Betriebssystem enthalten, während Outlook meist mit dem Office-Paket geliefert wird. Alternativ gibt es noch Mozilla Thunderbird.
Virenschutz	Unbedingt notwendig ist ein Virenschutz der regelmäßig (am besten automatisch) aktualisiert wird.
Drucker: Tintenstrahldrucker; alternativ Laserdrucker Netzwerkfähiger Laserdrucker	Welche Druckerart man wählt hängt von der Art und der Menge der zu druckenden Dokumente ab. Tintenstrahldrucker sind in der Anschaffung günstig und bieten die Möglichkeit, farbige Ausdrucke zu machen. Allerdings sind die Druckkosten pro Seite relativ teuer, speziell bei Farbdrucken. Sie eignen sich somit für gelegentliche Ausdrucke mit farbigen Elementen. Laserdrucker bieten erst bei teureren Modellen Farbdrucke. Die kleineren Monochrom-Modelle eigenen sich vor allem für kleine bis mittlere Druckvolumina, die keinen Farbdruck erfordern. Die Kosten pro Seite sind deutlich geringer als bei Tintenstrahldruckern.
Printserver	Bei Peer-to-Peer vernetzen Rechnern bietet sich die Möglichkeit einen Laserdrucker mit kleinem Printserver einzusetzen. Dieser kann dann von allen angeschlossenen Rechnern genutzt werden. Meist handelt es sich dabei um einen leistungsfähigen Drucker der auch größere Ausdruck-Mengen ermöglicht.
Switch	Für die Peer-to-peer Vernetzung wird ein Switch benötigt der die einzelnen PCs verbindet. Dieser muss ausreichend Ports bieten um alle Geräte anzuschließen. Mit einzurechnen sind dabei evtl. vorhandene Netzwerkdrucker und Router. Switche sind heute mit bis zu 1 GBit/s Anschlüssen erhältlich. Allerdings reichen für den normalen Bürobetrieb Geräte mit 100 MBit/s vollständig aus.
Internet-Zugang Router mit integrierter Firewall	Um den Internetzugang für mehr als zwei PCs zu realisieren, empfiehlt es sich sowohl bei ISDN als auch bei DSL einen Router einzusetzen. Dieser baut die Internetverbindung stellvertretend für die Rechner auf und bei Nichtnutzung wieder automatisch ab. Wird der Internetzugang von mehr als einem Rechner genutzt, so teilen sich diese den Zugang über den Router automatisch. Für den Internetzugang stehen als Alternativen ISDN oder DSL zur Verfügung. ISDN ist zu empfehlen wenn nur gelegentlich Informationen aus dem Internet abgerufen werden. DSL rentiert sich bei Online-Zeiten von mehr als ca. 40 Std./Monat oder großen Download-Mengen, da hierfür sog. Flatrates verfügbar sind.

Gerät:	Bemerkung:
Funk-LAN	Funk-LANs bzw. Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen Aufgrund der bequemen Einrichtung der WLAN-Netze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA-Verschlüsselung einschalten (langes Kennwort) • Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
Zugang zum OKR-Netz: Zugangskennungen IP-Adressen	Auf den Rechnern des OKR werden neben der Bürokommunikation eine Reihe weiterer Anwendungen im Bereich Personalwesen, Finanzwesen u. a. angeboten. Der Zugang erfolgt üblicherweise über das Internet und das Produkt Citrix, das auf dem lokalen PC installiert wird. Die Zugangskennung vergibt das Referat IT. Für lokale Netzwerke sollten IP-Adressen verwendet werden, die das Referat IT zuweist.

3. Dienststellen mit bis 5 und mehr PCs:

Gerät:	Bemerkung:
PC(s) mit: • Prozessor Intel/AMD mit ca. 3GHz bzw. Dual Core Prozessoren • Hauptspeicher: 512 - 1024MB • Festplatte: 80 – 250 GB • Netzwerkkarte für Peer-to-Peer-Vernetzung • Microsoft Windows XP Professional • Microsoft Office XP oder 2003	Für die normale Bürotätigkeit reicht ein PC im mittleren Preissegment aus. Höhere Rechenleistung ist nur notwendig wenn häufig aufwendige Bildbearbeitung gemacht werden soll. Höchste Rechenleistung ist meist überproportional teuer. Für die Datensicherung bietet sich je nach Menge der Daten ein DVD oder CD-Brenner an, da diese eine einfache Handhabung sowohl bei Sicherung als auch bei der Wiederherstellung der Daten bieten. Als Betriebssystem sollte MS Windows XP Professional eingesetzt werden, da dieses stabil läuft und auch relativ viele Programme dafür verfügbar sind. Außerdem unterstützt der OKR momentan nur MS Win XP Professional (oder ältere MS Betriebssysteme) für seine Programme. Im Gegensatz zur Home-Variante ermöglicht Professional differenziertere Sicherheitseinstellungen und ermöglicht später auch eine professionelle Vernetzung. Für die Bürokommunikation empfiehlt es sich MS Office XP oder 2003 zu nehmen, da dies einen problemlosen Austausch von Dokumenten mit vielen anderen Dienststellen ermöglicht – MS-Office ist derzeit Defacto Standard.
E-Mail	Für E-Mail-Kommunikation stehen derzeit mehrere Programme zur Verfügung. Outlook Express ist kostenlos im Betriebssystem enthalten, während Outlook meist mit dem Office-Paket geliefert wird. Alternativ gibt es noch Mozilla Thunderbird.
Server mit: • Prozessor Intel/AMD mit ca. 3GHz • Hauptspeicher: 1024 – 2048 MB • Festplatte(n): 160 – 400 GB (evtl. RAID) • Band-Sicherungslaufwerk • Netzwerkkarte • Microsoft Windows Server 2003 alternativ Server 2003 Small Business Edition • Sicherungsprogramm • Zentraler Virenschutz	Beim Server handelt es sich um einen weiteren Rechner im Netzwerk, der aber nicht als Arbeitsplatz genützt wird, sondern zur zentralen Datenablage dient. Außerdem werden dort die Berechtigungen für das ganze Netzwerk verwaltet und die Sicherung der Daten gemacht. Mit einem zentralen Virenschutz auf dem Server ist ein automatisches Update der PCs möglich. Wird als Betriebssystem die "Small Business Edition" gewählt kann der Server auch als zentraler Mailserver genutzt werden. Zur Erhöhung der Ausfallsicherheit kann der Server mit mehreren Festplatten ausgerüstet und diese in einem RAID-Verbund zusammengeschaltet werden. Fällt dann eine Festplatte aus, kann der Server ohne Ausfall weiter betrieben werden. Für die Sicherung der Daten ist ein Bandsicherungslaufwerk mit passendem Sicherungsprogramm notwendig. Alternativ kann auch ein DVD-Brenner verwendet werden, der aber max. 8 GB sichern kann. Wichtig sind die Kontrolle des Sicherungsprogramms und die Auslagerung der Sicherungsmedien wegen evtl. Katastrophenfällen.
Drucker: Tintenstrahldrucker; alternativ Laserdrucker Netzwerkfähiger Laserdrucker	Welche Druckerart man wählt, hängt von der Art und der Menge der zu druckenden Dokumente ab. Tintenstrahldrucker sind in der Anschaffung günstig und bieten die Möglichkeit, farbige Ausdrucke zu machen. Allerdings sind die Druckkosten pro Seite relativ teuer, speziell bei Farbdrucken. Sie eignen sich somit für gelegentliche Ausdrucke mit farbigen Elementen. Laserdrucker bieten erst bei teureren Modellen Farbdrucke. Die kleineren Monochrom-Modelle eigenen sich vor allem für kleine bis mittlere Druckvolumina, die keinen Farbdruck erfordern. Die Kosten pro Seite sind deutlich geringer als bei Tintenstrahldruckern.
Printserver	Bei Peer-to-Peer vernetzen Rechnern bietet sich die Möglichkeit einen Laserdrucker mit kleinem Printserver einzusetzen. Dieser kann dann von allen angeschlossenen Rechnern genutzt werden. Meist handelt es sich dabei um einen leistungsfähigen Drucker der auch größere Ausdruck-Mengen ermöglicht.
Switch	Für die Peer-to-peer Vernetzung wird ein Switch benötigt der die einzelnen PCs verbindet. Dieser muss ausreichend Ports bieten um alles Geräte anzuschliessen. Mit einzurechnen sind dabei evtl. vorhandene Netzwerkdrucker und Router.

Gerät:	Bemerkung:
	Switche sind heute mit bis zu 1 GBit/s Anschlüssen erhältlich. Allerdings reichen für den normalen Bürobetrieb Geräte mit 100 MBit/s vollständig aus.
Internet-Zugang Router mit integrierter Firewall	Um den Internetzugang für mehr als zwei PCs zu realisieren, empfiehlt es sich sowohl bei ISDN als auch bei DSL einen Router einzusetzen. Dieser baut die Internetverbindung stellvertretend für die Rechner auf und bei Nichtnutzung wieder automatisch ab. Wird der Internetzugang von mehr als einem Rechner genutzt, so teilen sich diese den Zugang über den Router automatisch. Für den Internetzugang stehen als Alternativen ISDN oder DSL zu Verfügung. ISDN ist zu empfehlen wenn nur gelegentlich Informationen aus dem Internet abgerufen werden. DSL rentiert sich bei Online-Zeiten von mehr als ca. 40 Std./Monat oder großen Download-Mengen, da hierfür sog. Flatrates verfügbar sind.
Funk-LAN	Funk-LANs bzw. Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen. Aufgrund der bequemen Einrichtung der WLANNetze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA-Verschlüsselung einschalten (langes Kennwort) • Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
Zugang zum OKR-Netz: Zugangskennungen IP-Adressen	Auf den Rechnern des OKR werden neben der Bürokommunikation eine Reihe weiterer Anwendungen im Bereich Personalwesen, Finanzwesen u. a. angeboten. Der Zugang erfolgt üblicherweise über das Internet und das Produkt Citrix, das auf dem lokalen PC installiert wird. Die Zugangskennung vergibt das Referat IT. Für lokale Netzwerke sollten IP-Adressen verwendet werden, die das Referat IT zuweist.

Anlage 2: Software für externe Dienststellen

Diese Anlage enthält Empfehlungen zum Softwareeinsatz für kleine und mittlere Einrichtungen (in Ergänzung zum IT-Konzept und in Ergänzung zu der in Analage 1 beschriebenen Hardware-Ausstattung).

Auch hier wird zunächst der für den geordneten Ablauf in einer Dienststelle benötigte Softwarebedarf beschrieben, darüber hinaus werden aber auch Empfehlungen für Programme ausgesprochen, die in kleineren und mittleren Dienststellen von der gegenüber großen Einrichtungen anderen Aufgabenstellung her benötigt werden (z. B. Gemeindebaukasten). Außerdem sind hier in Ergänzung zu den Ausführungen in Kapitel XI Datenschutz und Datensicherheit die als Freeware oder Shareware erhältlichen Programme zur Unterstützung der täglichen Arbeit aufgeführt.

Anmerkung: Windows Vista und Office 2007 sind neue Softwareprodukte der Firma Microsoft. Gegenwärtig unterstützt Windows Vista noch nicht alle Anwendungsprogramme unserer Landeskirche (z. B. Kifikos). Insbesondere im Modul Powerpoint und im Makrobereich sollte zurzeit mit Kompatibilitätsproblemen gerechnet werden, die sich durch spezielle Tools von MS nicht vollständig beseitigen lassen. Aus diesen Gründen wird gegenwärtig nicht empfohlen Windows Vista und Office 2007 umgehend einzusetzen. Es wird an dieser Stelle ausdrücklich darauf hingewiesen, dass es sich hierbei um eine vorläufige Empfehlung handelt.

1. Betriebssysteme

Software	Kurzbeschreibung	Beschreibung/ Voraussetzungen
Windows Vista	Anfang des Jahres 2007 neu auf den Markt gekommen. Von einem sofortigen Einsatz wird dringend abgeraten, da die erforderlichen Gerätetreiber noch nicht in vollem Umfang zur Verfügung stehen und eine Reihe von Anwenderprogrammen auf dieses neue Betriebssystem noch nicht angepasst sind.	Kommerzielle Software Systemvoraussetzung: Pentium IV bzw. Dual Core Prozessoren oder vergleichbare Prozessoren von AMD Speicher 1024 MB RAM
Windows XP Pro	Zurzeit Standard bei neuen PCs. Falls bei Auslieferung nur WIN XP home enthalten ist, wird die Aufrüstung auf WIN XP Pro empfohlen.	Kommerzielle Software Systemvoraussetzung: Pentium III oder höher bzw. vergleichbare Prozessoren von AMD Speicher mind. 256 MB RAM empf. 512 MB RAM
Windows 2000	Standard für vorhandene Personalcomputer	Kommerzielle Software Systemvoraussetzung: Pentium III oder höher bzw. vergleichbare Prozessoren von AMD Speicher mind. 128 MB RAM empf. 256 MB RAM

2. Office-Anwendungen

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
MS Office 2007	Anfang des Jahres 2007 neu auf den Markt gekommen. Von einem sofortigen Einsatz wird abgeraten, da mit größeren Umstellungsarbeiten vor der Benutzung des Programms gerechnet werden muss. Dies gilt sowohl für einen erhöhten Schulungsbedarf, weil die Benutzung der Software vom Hersteller angepasst wurde als auch bei der Kommunikation mit den Vorgängerversionen.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/VISTA
MS Office 97 bis 2003	Standardmäßig verwendetes Officesystem. Ab Office 2003 werden Windows 2000 oder XP vorausgesetzt.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/Vista
OpenOffice	Leistungsfähiges Officepaket. Der Einsatz ist bisher nicht erprobt. Die Übernahme von Dateien zwischen Microsoft Office und Open Office erfolgt nicht immer fehlerfrei.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/Vista/LINUX

3. Web Browser

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
MS Internet Explorer	Weit verbreiteter Internetbrowser. Weiterentwicklung nur noch für WIN 2000 und XP	Freeware Systemvoraussetzung: WIN 2000/XP/Vista
Mozilla Firefox	Alternative zum Internet Explorer.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/Vista/LINUX
Opera	Alternative zum Internet Explorer.	Freeware Systemvoraussetzung: WIN 2000/XP

4. Mail Server

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
Microsoft Exchange	Server für die zentrale Verwaltung von Mails, Terminen und Kontakten. Setzt einen Server voraus; auch als Paket Microsoft Small Business Server erhältlich.	Kommerzielle Software Systemvoraussetzung: WIN 2000/2003 Server
AVM KEN!3	Einfacher Mail-, Proxy und CAPI-Server für kleinere Netzwerke	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/2003
JanaServer	Einfacher Mail- und Proxy-Server für kleinere Netzwerke	Kostenlos für nichtkommerziellen Einsatz Systemvoraussetzung: WIN 98SE/2000/XP

5. Firewall, Virenscanner, Antispyware

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
Symantec Norton Internet Security	Firewall und Virenscanner (auch als reiner Virenscanner erhältlich: Norton AntiVirus)	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
Mcafee Internet SecuritySuite	Firewall und Virenscanner (auch als reiner Virenscanner erhältlich: virusscan)	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
H+BEDV AntiVir PersonalEdition Classic	Virenscanner	Freeware Systemvoraussetzung: WIN 98SE/2000/XP
ZoneAlarm	Firewall; bietet erweiterte Möglichkeiten gegenüber der Windows XP-Firewall	Kostenlos für nichtkommerziellen Einsatz Systemvoraussetzung: WIN 98SE/2000/XP
Windows XP-Firewall	Firewall. Diese einfache Firewall ist bereits kostenlos im Betriebsystem enthalten.	kostenlos Systemvoraussetzung: WIN XP
Ad-Aware Personal	Software zum Auffinden und löschen von unerwünschten Programmen (Spyware).	Kostenlos für nichtkommerziellen Einsatz Systemvoraussetzung: WIN 98SE/2000/XP
Search & Destroy	Software zum Auffinden und löschen von unerwünschten Programmen (Spyware).	Freeware Systemvoraussetzung: WIN 98SE/2000/XP

6. Anwenderprogramme

6.1. Bildbearbeitung

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
IrfanView	Einfaches und übersichtliches Bildbearbeitungsprogramm mit Batchkonvertierung aber eingeschränktem Funktionsumfang	Freeware Systemvoraussetzung: WIN 98SE/2000/XP
Gimp	Leistungsfähiges aber nicht besonders übersichtliches Bildbearbeitungsprogramm.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/LINUX
Photoshop	Leitungsfähiges und weit verbreitetes Bildbearbeitungsprogramm.	Kommerzielle Software Systemvoraussetzung: WIN 2000/XP/Vista

6.2. Präsentation und Projektarbeit

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
MS PowerPoint	Weit verbreitetes Standardprogramm für Präsentationen mit Beamer.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/Vista
Impress (OpenOffice)	Äquivalent zu MS Powerpoint. Der Einsatz ist bisher nicht erprobt. Die Übernahme von Dateien zwischen Microsoft Powerpoint	Open Source Systemvoraussetzung:

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
	und Impress erfolgt nicht immer fehlerfrei.	WIN 98SE/2000/XP/Vista/LINUX
Mind Manager oder Openmind	Einfach zu handhabende Programme zur übersichtlichen Darstellung von Zusammenhängen.	Kommerzielle Software Systemvoraussezung: WIN 98SE/2000/XP
MS Project	Werkzeug zur Planung und Kontrolle umfangreicher und komplexer Projekte.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/Vista
GanttProject	Werkzeug zur Planung und Kontrolle mittlerer und komplexer Projekte.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/LINUX

6.3. Personalwesen

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
pcBAT TVöD	Als Ergänzung der Software im Bereich Personalwesen empfohlen.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Gehaltsrechner: gehalt.de	Als Ergänzung der Software im Bereich Personalwesen einsetzbar.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Lexware lohn + gehalt	Als Ergänzung der Software im Bereich Personalwesen einsetzbar.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Haufe TVöD - Office	Informationssystem für die BAT-Personalarbeit	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Haufe– Personal Office	Informationssoftware für den Personalbereich	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
SV.Net	Erstellung und Übermittlung von Sozialversicherungsmeldungen und Beitragsnachweise an die Krankenkassen.	kostenlos Systemvoraussetzung: WIN 98SE/2000/XP

7. Utilities

7.1. Packprogramme

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
WinZip	Komfortables und weit verbreitetes Programm zum Packen und Entpacken von Dateien bzw. Verzeichnissen.	Shareware Systemvoraussetzung: WIN 98SE/2000/XP
Power Archiver 2000	wie oben	Freeware Systemvoraussetzung: WIN 98SE/2000/XP
Power Archiver 2007	wie oben	Shareware Systemvoraussetzung: WIN 98SE/2000/XP/VISTA

7.2. Backup

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Veritas Backup Exec	Software zur automatisierten Sicherung von Servern und deren Diensten	Kommerzielle Software Systemvoraussetzung: WIN 2000/2003
Windows Sicherungsprogramm	Software zur Sicherung von Daten auf Einzelplatz-Rechner und Server	Kostenlos im Betriebssystem enthalten Systemvoraussetzung: WIN 2000/XP/2003
Backup Slave	Backup auch auf externe Laufwerke (auch Sticks) und Brenner möglich.	Freeware Systemvoraussetzung: WIN 98SE/2000/XP

7.3. Brennsoftware

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Nero	Einfach zu bedienendes Programm zum Brennen von CDs und DVDs.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/VISTA/LINUX
Burn4Free	Einfaches Brennprogramm für CDs und DVDs.	Freeware Systemvoraussetzung: WIN 98SE/2000/XP

7.4. Viewer

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Adobe Reader	Programm zum Anzeigen und Drucken von PDF-Dateien sowie zum Suchen in diesen Dateien.	Freeware Systemvoraussetzung: WIN 98SE/2000/XP/VISTA/LINUX

7.5. PDF-Konverter

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
FreePDF XP	Umwandlung beliebiger Anzeigeformate in PDF-Dateien(auch Word, Excel, usw.). Zusammenfügen mehrerer PDF-Dateien zu einer Datei.	Freeware Systemvoraussetzung: WIN 2000/XP

7.6. HTML-Editor

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Gemeindebaukasten	Einfach zu handhabender Softwarebaukasten zum Erstellen von Internetseiten.	Software vom Evangelischen Medienhaus Stuttgart zusammengestellt Systemvoraussetzung: WIN 98SE/2000/XP

Anlage 3: Preisliste für Leistungen im Referat Informationstechnologie

-Stand November 2012-

Leistung	EURO	
	einmalig	lfd.
Full - Service Basisdienste / Betreuung Standard Arbeitsplatz OKR: (Monatspauschale pro E-Mail Postfach) Systemzugang, Systemaktualität, Software-Paketierung (Standard SW), automatisierte Softwareverteilung, Datensicherung, Systemsicherheit inkl. Viren- & Spamschutz, Homeshare, Gruppenshare, Infosystem, Telefon-Support, Helpdesksystem, Infrastruktur OKR, Netzwerkmanagement		130,00
Betreuung angeschlossene externe Dienststellen (OKR Server) (Monatspauschale / E-Mail Postfach) Systemzugang, Systemaktualität, Software-Paketierung (Standard SW), automatisierte Softwareverteilung, Datensicherung, Systemsicherheit inkl. Viren- & Spamschutz, Telefon-Support Helpdesksystem, Infrastruktur OKR, Netzwerkmanagement		70,00
Betreuung Dienststellen mit eigenen Server (Monatspauschale / E-Mail Postfach) Bereitstellung eines redundanten Internetzugangs über die Systemumgebung des OKR, Zentraler Virenschutz für einkommende E-Mails, Spamfilter für einkommende E-Mails, Kontaktintegration in Outlook, Empfang / Versand / Weiterleitung E-Mails an die Dienststelle, Telefon-Support.		13,00

Leistung	EURO	
	einmalig	lfd.
Web Hosting: (Monatspauschalen)		
Einrichten eines benutzerspezifischen Bereichs in unserem Rechnerumfeld, Bereitstellung von bis zu 10 (zehn) MByte auf unserem WWW-Server, FTP Zugang mit Kennwort zur Aktualisierung & Pflege der vorhandenen Daten, Festlegen einer Internetadresse in unserem Bereich ("www.name.elk-wue.de"); Skriptsprache PHP; Bei Bedarf Einrichtung einer E-Mail-Weiterleitung; Zugriffstatistik; Betrieb des virtuellen Servers durch 24 h x 7 Tage Überwachung		14,50
Administration des Vorgangs, Dokumentation, einmaliger Einrichtungsaufwand	60,00	
Je weitere 5 (fünf) MByte Speicherplatz auf WWW-Server		0,50
Eigene Domain		
- einmalig	50,00	
- jährlich		30,00
Unterstützung der Seitengestaltung durch das Evangelischen Medienhaus	nach Aufwand	
Betrieb BlackBerry/Handheld (Monatspauschale)		
BlackBerry Software und Installation auf Serverumgebung der Referat Informationstechnologie. Bereitstellung einer PC-Synchronisationssoftware für den Desktop, Betreuung.		13,75
Zusätzlich: Laufende Ausgaben an den Mobilfunkanbieter richten sich nach den dort geltenden Tarifen.		
Software		
combit Relationship Manager (cRM) (Adressverwaltung)	auf Anfrage	

Leistung	EURO einmalig	EURO lfd.
Fachanwendungen EDV-Finanzmanagement		
<u>CuZea:</u>		
- Erwerb pro Lizenz	150,00	
- Produktion und Betreuung pro Jahr erfolgt im Rahmen der Abrechnung Navision-K (siehe unten)		
<u>Navison für kfm. Einrichtungen (Produktion und Betreuung):</u>		
- pro Mandant /Jahr		240,00
- pro User /Jahr		360,00
<u>Navison-K (Produktion und Betreuung):</u>		
- Sockelbetrag pro Mandant / Jahr		275,00
- pro 1.000 € Volumen des Ordentlichen Haushalts / Jahr (Volumen ohne Abschreibungen, Innere Verrechnungen, Zuführung an VMH etc.).		0,98
Anmerkung: Die maximalen Kosten pro Mandant und Jahr werden bei 6.875 € (= 25 x Sockelbetrag) gedeckelt. Die oben genannten Preise gelten nicht für Dienststellen im Oberkirchenrat.		
<u>Navison-K (Produktion und Betreuung) für Dienststellen im Oberkirchenrat:</u>		auf Anfrage
Fachanwendungen Meldewesen		
<u>DAVIP-W / AHAS - Lizenzen:</u>		
- Kirchengemeinden unter 2.500 Gemeindeglieder	150,00	
- Kirchengemeinden über 2.501 Gemeindeglieder	250,00	
- Unterlizenz im Bereich einer Kirchengemeinde	100,00	
- Bezirkslizenz AHAS	auf Anfrage	
<u>DAVIP-W / AHAS - (Produktion und Betreuung):</u>		
- Kirchengemeinden unter 2.500 Gemeindeglieder (pro Jahr)		35,00
- Kirchengemeinden über 2.501 Gemeindeglieder (pro Jahr)		50,00
- Unterlizenz im Bereich einer Kirchengemeinde (pro Jahr)		35,00
Fallpreis Meldewesenverarbeitung pro Gemeindeglied/Jahr		0,39

Leistung	EURO	
	einmalig	lfd.
Fachanwendung EDV-Personalmanagement		
Personal Office Grundmodul:		
Gehaltsabrechnung einschl. PO-Connect		
- Einzelplatz pro User /Monat		26,00
- bei 2-5 Plätzen pro User /Monat		23,00
- ab 6 Plätzen pro User /Monat		22,00
Personal Office Bescheinigungswesen		
pro User /Monat		18,00
Personal Office Stellenplan		
pro User /Monat		23,00
Personal Office Urlaubs- und Fehlzeitenverwaltung		
- Einzelplatz pro User /Monat		15,00
- ab 2 Plätzen pro User /Monat		13,00
Personal Office Weiterbildungsverwaltung		auf Anfrage
pcBAT TVöD		
pro User /je Update (i. d. R. 2-3 pro Jahr)		30,00
Haufe TVöD-Office		
pro User /Jahr		90,00
Haufe Personal Office		
pro User /Jahr		90,00
Microview		auf Anfrage
LDMS		auf Anfrage
Geographisches Informationssystem (Beispiel Pfarrstellenkarte)		auf Anfrage

Leistung		EURO einmalig	EURO lfd.
Schulungen			
Schulungen MS-Office Produkte -	½ Tag pro Person	65,00	
Schulungen MS-Office Produkte -	1 Tag pro Person	130,00	
Schulungen zu diversen Themen: Datensicherheit, Internet, WLan, Netzwerk, Datenaustausch, Spamschutz,... (siehe Schulungsangebote des Referats Informationstechnologie)	1 Tag pro Person	130,00	
Navision-Schulungen im OKR	1 Tag pro Person	90,00	
Navision-Schulungen im OKR	½ Tag pro Person	45,00	
DaviP-W Grundkurs/Aufbaukurs	1 Tag pro Person	60,00	
Schulungsraummiete in den Räumen des Referats IT			
Präsentations-/ Schulungsraum (ohne Referent) (11 PC-Arbeitsplätze, inkl. Lehrer PC, Video Beamer) – pro Tag: *Mengenrabatt: 5 Tage, 15% / 10 Tage, 20% / 25 Tage, 25%*		350,00	
Schulungsreferent	1 Tag Pauschal	720,00	
	½ Tag Pauschal	400,00	
	Stundensatz (bis 2 Std.)	90,00	
Bei Einsatz des Mobilen Schulungsraums berechnen wir zusätzlich einen einmaligen Aufschlag für Auf- und Abbau ...		350,00	
Beamermiete (1.500 Ansi-Lumen SVGA) pro Tag:			
1-2 Tage		50,00	
3-4 Tage		45,00	
ab 5 Tage		40,00	
Verleih an Dienststellen innerhalb des Oberkirchenrats (je angefangener ½ Tag)		15,00	
Personenstundensatz Referat Informationstechnologie			
Beratung, Analyse, Einweisung, Programmerstellung /pro Stunde		60,00	

Leistung	EURO	
	einmalig	lfd.
Reisekosten / Reisezeiten		
Pauschale	75,00	
In der angegebenen Fahrtkostenpauschale sind alle KFZ-, Reisekosten und Anfahrtszeiten (Hin- und Rückfahrt) enthalten.		
Beschaffung von Hardware		
Beschaffung von Hardware (PCs, Drucker, Scanner, ect.)	nach Aufwand	
Bei Beschaffung von Notebooks und PCs ist eine Finanzierung über mehrere Jahresraten möglich:		
aktuelle Finanzierungsraten:		
- pro PC und Jahr (4 Jahresraten)	370,00	
- pro Notebook und Jahr (3 Jahresraten)	810,00	
PC - Installationspauschale (Erstinstallation - inkl. Rollout)	200,00	
Nebenkosten		
Zusätzliche Kosten und ggf. anfallende Übernachtungskosten werden (nach Beleg) separat abgerechnet.	nach Aufwand	

Diese Preisliste gilt zusammen mit den Allgemeinen Geschäftsbedingungen IT und einer konkreten Service-Vereinbarung zwischen dem Auftraggeber und dem Referat IT, welche die Art und den Umfang der zu erbringenden Leistungen beschreibt.

Anlage 4: Abkürzungsverzeichnis

Abkürzung	Bedeutung
AD	Active Directory
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ASP	Active Server Page oder Application Service Providing
ATM	Asynchronous Transfer Mode
BK	Bürokommunikation
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAD	Computer Aided Design
CASE	Computer Aided Software Engineering
CD ROM	Compact Disk Read only Memory
CERT	Computer Emergency Response Team
CE	Communauté Européenne
COM	Component Object Model
CORBA	Common Object Request Broker Architecture
COS	Common Object Services
C/S	Client-Server
DB	Datenbanken
DBMS	Datenbank Management System
DCOM	Distributed Component Object Modell
DDE	Dynamic Data Exchange
DDL	Data Definiton Language
DES	Data Encryption Standard
DML	Data Manipulation Language
DNS	Domain Name Service
DSA	Directory Service Agent oder Digital Signature Algorithmus
DSS 1	Digital Subscriber Signaling System No.1
DTD	Document Type Definition
DV	Datenverarbeitung
DVD	Digital Versatile Disc
DXF	Drawing Exchange Format
ECC	Elliptic Curve Cryptography
ECMA	Verband der europäischen Computerhersteller (European Computer Manufacturers Association)
EDS	Electronic Data Systems
e-GK	e-Government-Konzept (vormals Landessystemkonzept des Landes Baden-Württemberg)
EJB	Enterprise Java Beans
EMV	Elektromagnetische Verträglichkeit von Geräten
EMVG	Gesetz über die elektromagnetische Verträglichkeit von Geräten

Abkürzung	Bedeutung
EN	Europäische Norm
ERD	Entity Relationship Diagram
ERM	Entity Relationship Modell
ESMTP	Enhanced Simple Mail Transfer Protocol
ESP	Encapsulating Security Payload
ETS	European Telecommunication Standard
ETSI	Europäisches Normierungsinstitut auf dem Gebiet der Telekommunikation (European Telecommunication Standards Institute)
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
GIS	Geografisches Informationssystem
GML	Geographic Markup Language
GNU	General Public License
GSM	Global System for Mobile Communication
HTML	Hypertext Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICA	Independent Computing Architecture
IDE	Integrated Development Environment
IDEA	International Data Encryption Standard
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronical Engineers
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IKE	Internet Key Exchange
IMAP	Internet Mail Access Protocol
IP	Internet Protocol
IPsec	Internet Protocol Secure
IPv4 / IPv6	Internet Protocol Version 4 / Version 6
ISAKMP	Internet Security Association Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Standardization Organisation
IT	Informations-Technologie
ITSM	IT-Service Manager (Problem-Management-Software von Hewlett Packard)
ITO	IT/Operations
ITU (-TS)	International Telecommunication Union (-Telecommunication Standards)
IuK	Informations- und Kommunikationstechnik, Information und Kommunikation
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
JPEG	Joint Photographic (Coding) Experts Group (Standard-Kodierung für digitale Fotos)
JScript	Java Script
JSP	Java Server Pages
KRZ-SWD	Kirchliches Rechenzentrum Südwestdeutschland
LAN	Lokales Netzwerk (Local Area Network)
LDAP	Light Weight Directory Access Protocol

Abkürzung	Bedeutung
LSK	Landessystemkonzept des Landes Baden-Württemberg (jetzt e-Government-Konzept)
MailTrusT	Bund-Länder-Standard für die Verschlüsselung von Mails
MIB	Management Information Base
MDX	Multidimensional Expression
MIME	Multipurpose Internet Mail Extensions
MHS	Message Handling System
MPR	Mät och Prov Rådet II
MS	Microsoft
MTA	Message Transfer Agent
MTT	MailTrust
MVS	Multiple Virtual System
NAS	Normierte Austauschschnittstelle (EDBS-Nachfolge)
NC	Network Computer
NIST	National Insitute of Standards and Technology
NNTP	Network News Transfer Protocol
NTP	Network Time Protocl
NT	Betriebssystem der Fa. Microsoft (New Technology)
ODBC	Open Data Base Connectivity
ODMG	Object Database Management Group
OGIS	Open GIS
OGC	Open GIS Consortium
OMG	Object Management Group
OLAP	On-Line Analytical Processing
OLE	Object Linking and Embedding
OO	Object Orientiert
OQL	Object Query Language
ORB	Object Request Broker
OS	Operating System
OSI	Standardisierungsarchitektur für offene Systeme (Open Systems Interconnection)
OSS	Open Source Software
PC	Personal Computer
PCL	Printer Control Language
PDF	Portable Document Format
PEM	Privacy Enhanced Mail
PERL	Practical Extraction and Report Language
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PM	Projektmanagement
POP	Point of Presence oder Post Office Protocol oder Prozeßoptimierung im Personalwesen
POSIX	Portable Operating System Interface
PSS1	Private Signalling System Nr. 1
QoS	Qualtiy of Services

Abkürzung	Bedeutung
QSIG	Q-Interface Signalling Protocol
RAD	Rapid Application Development
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol
RFC	Request for Comment
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RSA	Rivest, Shamir und Adleman
RSVP	Resource Reservation Protocol
RTF	Rich Text Format
SAGA	Standards und Architekturen für E-Governement-Anwendungen
SDK	Software Development Kit
SGML	Standard Generalized Markup Language
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	System Management Services
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	SimpleNetwork Time Protocl
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
S/STP	Shielded/Shielded Twisted Pair
TC	Technical Committee oder Trust Center
TCO	Total Costs of Ownership
TCO	Tjäntemännens Central Organisation
TCP	Transmisson Control Protocoll
TIFF	Tagged Image File Format
TK	Telekommunikation
TLS	Transport Layer Security
TSE	Terminal Server Edition
UA	User Agent
UDT	User Defined Types
URL	Uniform Resource Locator
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
VB	Visual Basic
VBA	Visual Basic for Applications
VBScript	Visual Basic Script
VPN	Virtual Private Network
VoIP	Voice over IP
W3C	World Wide Web Consortium
WAN	Weitverkehrsnetz (Wide Area Network)
WEP	Wired Equivalent Privacy (Verschlüsselungsprotokoll bei Funk-LAN)
WLAN	Wireless LAN oder Funk-LAN (drahtloses lokales Netzwerk)

Abkürzung	Bedeutung
WPA	Wireless Protected Access (Verschlüsselungsprotokoll bei Funk-LAN)
WWW	World Wide Web
XML	Extensible Markup Language
XP	Experience (neuestes Windows-Betriebssystem für Clients)
XSL	Extensible Stylesheet Language