Richtlinie Informationssicherheit und Datenschutz im Generalvikariat des Erzbistums Köln

Festlegung und Umsetzung von Informations-Sicherheits-Zielen und ihrer Anwendung zum Thema Datenschutz

Version: 1.0.

vom: 21.11.2013

Inhaltsverzeichnis

1. Geltungsbereich

Dieses Richtlinie zum Informationssicherheits- und Datenschutzmanagement ist für alle Mitarbeitenden, die im oder für das EGV arbeiten (auch Berater und Zulieferer) sowie für alle Stellen, von denen auf Daten oder Systeme des EGVs zugegriffen wird, gültig. Verantwortlich für die Umsetzung der beschriebenen Vorgaben sind primär Führungskräfte sowie Träger informationssicherheitsrelevanter Funktionen. Für die Einhaltung von Regeln und Anforderungen die insbesondere die EDV-Anwender betreffen, sind diese entsprechend selbst verantwortlich und in der Pflicht.

Das EGV betrachtet vorausschauendes Informationssicherheits- und Datenschutzmanagement als eine wichtige Führungsaufgabe, die sowohl die Entwicklung der Leitideen als auch die Verantwortung für die Informationssicherheits- und Datenschutzpolitik umfasst. Ziel ist, den IT-Einsatz und die elektronische sowie manuelle Datenverarbeitung jeglicher Art so zu lenken und kontinuierlich weiterzuentwickeln, dass potenzielle Risiken eingeschätzt und kontrolliert werden können. Dieser ganzheitliche Ansatz gewährleistet, dass die Anforderungen der einzelnen Abteilungen und deren Wechselbeziehungen berücksichtigt werden.

Dabei ist der Gedanke leitend, dass Informationen einen Wert für die Dienst- und Geschäftstätigkeit darstellen und durch unbefugte Kenntniserlangung, Verlust oder Verfälschung dieser Informationen dem EGV Schaden entstehen kann. In diesem Sinne sprechen wir von Informationssicherheitswerten in Bezug auf sämtliche Informationen aus:

- Daten und Datenbeständen
- Anwendungen und Datenbanken
- Systemen
- Kommunikationsvorgängen
- organisatorischen Abläufen

In Anlehnung an die Sicherheitsstandards ISO/IEC 27001:2005 umfasst die Richtlinie die folgenden Organisationsbereiche:

- Informationssicherheits- und Datenschutzpolitik und Organisation der Sicherheit
- Verwaltung von Informationswerten
- Personelle Sicherheit
- Physikalische und umgebungsbezogene Sicherheit
- Management des Betriebes und der Kommunikation
- Sicherheit der Zugänge zu Informationen
- Beschaffung, Entwicklung und Wartung von Informationssystemen

- Umgang mit Informationssicherheitsvorfällen
- Kontinuierliche Fortführung des Dienst- und Geschäftsbetriebes
- Datenschutz- und Konformitäts-Überprüfung

2. Organisation der Informationssicherheit

Verantwortlich für den Aufbau und die Aufrechterhaltung des Informationssicherheits- und Datenschutzmanagements ist der Zentrale Informationssicherheitsbeauftragte des EGVs (ZISB), der in seiner Tätigkeit durch ein Sicherheits-Team unterstützt wird. Der ZISB ist verantwortlich für die Erstellung sämtlicher Richtlinien, Konzepte und Maßnahmen, die sich aus den Anforderungen dieser Richtlinie ergeben. Zudem wacht er über die Einhaltung der Vorgaben des Informationssicherheits- und Datenschutzmanagements. Der ZISB muss über die notwendige Fachkunde zur Erfüllung seiner Aufgaben verfügen.

Der ZISB übernimmt die folgenden Aufgaben:

- Leitung des Sicherheits-Teams
- Entwurf und Entwicklung von Richtlinien und Konzepten zur Optimierung und Fortentwicklung des Informationssicherheits- und Datenschutzniveaus
- Kommunikation mit allen Organisationseinheiten und Einrichtungen zur gemeinsamen Umsetzung der getroffenen Regelungen
- Bewertung umgesetzter und geplanter Projekte vor allem im Bereich DV
- Sensibilisierung der Mitarbeitenden zu Informationssicherheitsthemen durch kontinuierliche Information und regelmäßige Schulung
- regelmäßige Überwachung und Auditierung der Datenverarbeitung im EGV
- regelmäßige Auditierung und Kontrolle der Auftragsnehmer des EGVs im Hinblick auf Informationssicherheitsanforderungen
- Regelmäßige Durchführung einer Risikoanalyse und Entwicklung risikogesteuerter Gegenmaßnahmen
- Abstimmung der Anforderungen mit der Diözesandatenschutzbeauftragten
- Funktion als erste Anlaufstelle für sämtliche Anfragen im Bereich der Informationssicherheit

Das Informationssicherheits- und Datenschutzmanagement des EGVs besteht aus einem Team unter Beteiligung der Referate DV-Service, Organisation sowie der Datenschutzverantwortlichen (Sicherheits-Team). Dieses Team kann fallweise um Mitglieder aus verschiedenen Abteilungen ergänzt werden. Die Abteilungen und Referate bleiben für die Beurteilung des Schutzbedarfs sowie für die Umsetzung der beschlossenen Richtlinien und Prozesse verantwortlich.

Ein weiteres wesentliches Element des Informationssicherheits-Management ist das Security-Board. Dieses Gremium behandelt alle sicherheits-relevanten Themen, die auch den IT-Service-Dienstleister betreffen. Neben dem ZISB ist hier mindestens noch der IT-Sicherheits-Beauftragte des jeweiligen Dienstleisters vertreten.

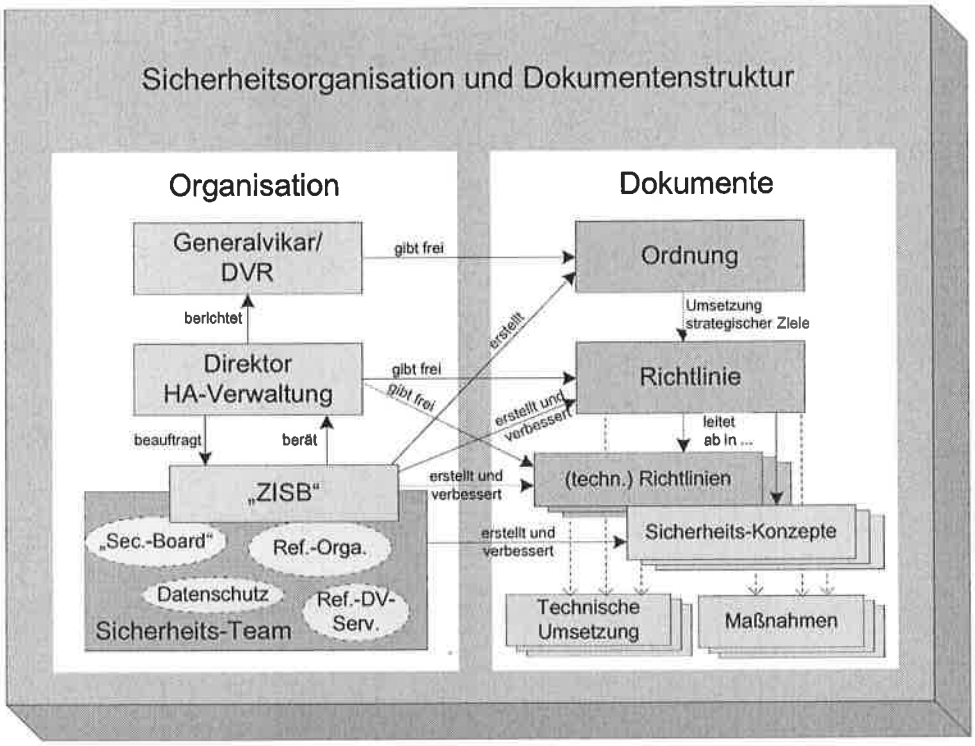

Abbildung 1: Organisation der Informationssicherheit

3. Verwaltung von Informationswerten

Damit das EGV gezielt Werte (Informationen, Software oder Hardware, der ein Wert für die Dienst- und Geschäftstätigkeit im EGV zukommt) schützen kann, sind ein umfassendes Werte-Inventar und eine Zuweisung von Verantwortlichkeiten für Werte

zwingend erforderlich. Zudem müssen Informationswerte entsprechend ihren Vertraulichkeitsstufen angemessen gekennzeichnet und gehandhabt werden.

3.1. Inventar der Werte

In Abstimmung mit dem Referat DV-Service führt der zuständige IT-Dienstleister ein Inventar sämtlicher im Auftrag eingesetzter Hardware- und Software-Werte. Das Referat DV-Service verwaltet die eingekauften Lizenzen und gleicht diese regelmäßig mit dem Inventar des Dienstleisters ab. Zudem überprüft das Referat DV-Service die Inventar-Liste des Dienstleisters regelmäßig stichpunktartig auf die Korrektheit der Einträge.

Ein aktuelles Inventar mit Hervorhebung aller Änderungen stellt der IT-Dienstleister dem Referat DV-Service monatlich sowie auf Anfrage zur Verfügung. Das Inventar umfasst die Art der Hardware oder Software, den Standort sowie die verantwortliche Person (bei Servern genügt ein Administrator, bei Clientsystemen ist die Angabe des Arbeitsplatzes / Büros erforderlich). Andere Wege der Hardware- und Softwarebeschaffung werden durch eine Integration der Inventarisierung in den Beschaffungsprozess berücksichtigt.

Datenbanken sowie datenhaltende Applikationen sind durch das Referat DV-Service zu inventarisieren.

Jede Art der Ausstattung darf nur im Rahmen ihres vorgesehenen Zweckes verwendet werden. So dürfen fest installierte Geräte (z.B. PCs, Drucker) nur von entsprechendem Fachpersonal auf- bzw. abgebaut werden, und für mobile Geräte (z.B. Notebooks, Smartphones) gilt für die Anwender eine besondere Sorgfaltspflicht.

3.2. Klassifizierung von Informationen

Die Klassifizierung von Informationen ist ein wesentliches Element sicherer Dienst- und Geschäftsprozesse, da die jeweils korrekte Handhabung von Informationen und Datenträgern jeglicher Art an die Vertraulichkeitsanforderungen gebunden ist. Grundsätzlich liegt die Verantwortung für die Klassifizierung in den einzelnen Fachbereichen, in denen die Daten erhoben bzw. bearbeitet werden. Die folgenden Klassifizierungsstufen wurden für das EGV festgelegt:

3.2.1. Öffentliche Informationen (niedriger Schutzbedarf):

Wenn Daten von der jeweils verantwortlichen Stelle für die Öffentlichkeit freigegeben wurden und keine weiteren Schutzmaßnahmen erforderlich sind, handelt es sich um öffentliche Information. (z.B. veröffentlichte Pressemitteilung, Amtsblatt, Informationen auf der Internetseite, Informationsbroschüren,...).

Nach der Freigabe sind an öffentliche Informationen keine Handlungsanweisungen gebunden.

3.2.2. Interne Informationen (mittlerer Schutzbedarf)

Wenn die Daten für den internen Gebrauch bestimmt sind und ihre unkontrollierte Weitergabe nur geringfügigen Schaden verursachen kann, handelt es sich um interne Informationen (z.B. interne Rundschreiben, Geschäftsverteilungspläne, Protokolle von Versammlungen mit breitem Teilnehmerkreis). Alle Informationen, die im EGV erstellt werden, gelten als intern, bis sie freigegeben oder höher klassifiziert werden.

Schutzmaßnahmen müssen sicherstellen, dass diese Daten nicht unkontrolliert veröffentlicht werden. Es ist untersagt, interne Informationen unkontrolliert an Dritte weiterzugeben, die Weitergabe an andere Parteien, die mit dem Informationsinhalt in Bezug stehen, bleibt davon unberührt. Bei Mailversand ist darauf zu achten, dass interne Informationen nicht auf unverifizierte, öffentliche E-Mail-Accounts (nicht personenbezogene, i.d.R. über Websites erreichbare Adressen oder an Mailinglisten) versandt werden. Das setzt voraus, dass sich der Absender über die Personen, die die verwendeten Adressen benutzen, vergewissert hat.

3.2.3. Vertrauliche Informationen (hoher Schutzbedarf)

Wenn der Zugriff auf die Daten aufgrund ihres Informationsgehaltes auf bestimmte Gruppen eingeschränkt werden muss, handelt es sich um vertrauliche Informationen. Eine Veröffentlichung dieser Daten würde zu mittleren Schäden für das EGV führen, wie z.B. bei Informationen über einen Teil des Dienstgeschäftes (z.B. grundsätzlich alle Akten in der Registratur, Kostenstellen-Strukturen) oder bei wichtigen Projektdokumenten. Aufgrund ihrer Einstufung sind diese Daten immer für festgelegte Bereiche freigegeben und können einzelnen Dritten gegenüber freigegeben sein.

Dritte, die Zugang zu diesen Informationen erhalten sollen, müssen eine Vertraulichkeitsvereinbarung unterzeichnen. Der Versand dieser Informationen in Emails außerhalb des EGV-Netzes hat stets verschlüsselt zu erfolgen. Bis auf weiteres sollte das als verschlüsselte Datei im Anhang erfolgen. Zur Verschlüsselung

kann hier das im Hause vorhandene Programm „*IZArc*“ verwendet werden. Office- oder PDF-Passwörter sind hierzu ungeeignet.

3.2.4. Streng vertrauliche Informationen (sehr hoher Schutzbedarf)

Wenn der Zugriff auf die Daten nur wenigen Personen erlaubt ist und die unkontrollierte Weitergabe der Daten sehr hohen Schaden anrichten kann, unterliegen diese Daten einem sehr hohen Schutzbedarf (z.B. höher klassifizierte Registratur-Akten, Personalakten).

Solche Informationen dürfen ausserhalb von klar definierten und gesicherten Prozessen grundsätzlich nicht elektronisch nach Extern weitergegeben werden.

Darüber hinaus ist die vollständige Sperrung von Akten möglich.

4. Informationssicherheit in den Personal-Verfahren

Die Mitarbeitenden des Generalvikariats sind wesentliche Träger des Informationssicherheits- und Datenschutzmanagements.

So sind schon bei der Personalgewinnung bestimmte Sicherheitsanforderungen zu berücksichtigen. Auch beim Ausscheiden von Mitarbeitenden muss zielgerichtet und schnell verfahren werden, um eventuelle Sicherheitslücken unmittelbar zu schließen. Dies gilt auch für Fremd-Mitarbeiter, die in den Räumlichkeiten und mit den Systemen des EGVs arbeiten.

Es soll sichergestellt werden, dass alle Mitarbeitenden sowie im Hause arbeitende Auftragnehmer unter Sicherheitsgesichtspunkten für ihre Stellen geeignet sind und ausreichend geschult sowie kontinuierlich sensibilisiert werden.

4.1. Vor Beginn des Dienstverhältnisses

Einzelne Rollen und Tätigkeiten im Generalvikariat können besondere Sicherheitsanforderungen notwendig machen. So sind Fachadministratoren nicht nur unter fachlichen Gesichtspunkten auszuwählen, sondern sollten auch Erfahrungen im Informationssicherheitsbereich mitbringen. Fachadministratoren sind all jene Mitarbeitenden, die aufgrund ihrer Tätigkeiten erweiterte Zugriffsrechte auf Datenbestände mit mindestens mittlerem Schutzbedarf haben, die zentrale

Applikationen oder Datenbanken administrieren oder für die Verwaltung von Rechten für die Anwender der Applikationen oder Datenbanken zuständig sind.

Für diese Stellen werden vom Referat DV-Service besondere Anforderungen definiert, die Bestandteil zukünftiger Stellenausschreibungen werden müssen. Gleiches gilt für Fachadministratoren im Bereich anderer verantwortlicher Stellen.

Vor der Einstellung eines neuen Mitarbeitenden in eine solche sicherheitskritische Rolle ist ein Screening durchzuführen. Die Screeningmaßnahmen umfassen u.a. auch:

- Stichprobenartige Kontaktaufnahme mit Referenzgebern ggf. unter Einbeziehung des betrieblichen Datenschutzbeauftragten und mit Einwilligung der Bewerber
- Anforderung des polizeilichen Führungszeugnisses als Bewerbungsunterlage

Als Bestandteil der Vertragsunterlagen müssen alle Mitarbeitenden in Voll- und Teilzeit, sowie gegebenenfalls alle externen Kräfte und temporäre Angestellte die Einhaltung der Regelungen dieses Informationssicherheits- und Datenschutzmanagementsystems anerkennen, sowie die Datenschutzerklärung unterzeichnen. Eine entsprechend notwendige Einweisung soll im Rahmen des allgemeinen Begrüßungsverfahrens („Einführungs-Veranstaltung") etabliert sein.

4.2. Während des Dienstverhältnisses

Alle Mitarbeitenden müssen geeignet ausgewählt und geschult sein, um die Anforderungen des Informationssicherheits- und Datenschutzmanagementsystems zu kennen und entsprechend konform handeln zu können. Hierzu sind insbesondere regelmäßige Sensibilisierungsmaßnahmen durchzuführen.

Sensibilisierungsmaßnahmen umfassen mindestens:

- einen Bereich im Intranet zu Informationssicherheits- und Datenschutzthemen
- Zielgruppen abhängige Schulungen zur Vermittlung von Wissen und zur Schaffung von Motivation bzw. Nachhaltigkeit

4.3. Änderung und Beendigung des Dienstverhältnisses

Im Falle des Wechsels eines Mitarbeitenden in eine andere Organisationseinheit sind die alten Rechte bis auf den Basis-Nutzer („Active-Directory"-Home-Verzeichnis und Outlook-Mail-Account) unverzüglich und vollständig zu löschen oder zu sperren. Neue Rechte auf Abteilungs-Verzeichnisse sowie spezielle Applikationen sind ausschließlich über die jeweiligen DV-Beauftragten durch die zuständige Abteilungsleitung zu beantragen. Die Aktivierung der neuen Rechte ist nur nach erfolgter Sperrung oder Löschung der alten Rechte zulässig. In begründeten Ausnahmen (bspw. Einarbeitung, Übergaben) können die alten Rechte zeitlich befristet beibehalten werden.

Eine Übersicht der Rechte des Basis-Nutzers sowie der abteilungsspezifischen Rechte des Mitarbeitenden wird zentral vom zuständigen IT-Dienstleister im Auftrag des Referates DV-Service sowie von den Fachadministratoren gepflegt. Begründete Ausnahmen und Abweichungen von diesem Verfahren werden vom Referat DV-Service dokumentiert und jährlich einer Überprüfung unterzogen.

Bei Beendigung des Arbeitsverhältnisses ist das Referat DV-Service unverzüglich durch die Personalabteilung zu informieren, so dass sämtliche Werte zurückverlangt werden können und sämtliche Rechte in Applikationen und Systemen gelöscht oder gesperrt werden können. Der Prozess ist nicht abgeschlossen, bevor diese Schritte nicht vollständig und dokumentiert durchgeführt wurden.

Mitarbeitende sind angewiesen, sämtliche Informationswerte des Generalvikariats zurückzugeben. Es dürfen keine Löschungen oder Manipulationen von Daten in den Systemen sowie auf dem Email-Account vorgenommen werden, soweit sie nicht im Rahmen der regulären Tätigkeit sowieso getätigt worden wären.

Bei außerordentlichen Kündigungen oder ordentlichen Kündigungen mit sofortigen Freistellungen ist ein separater beschleunigter Prozess unter Einbeziehung des zuständigen betrieblichen Datenschutzbeauftragten durchzuführen.

5. Physikalische und umgebungsbezogene Sicherheit

Die Regelung der physikalischen und umgebungsbezogenen Sicherheit dient dem Ziel, unbefugten und unsachgemäßen Zugriff auf EDV-Einrichtungen zu verhindern und die Verfügbarkeit, Integrität und Authentizität unserer Daten zu gewährleisten. Hierzu müssen die unterschiedlichen Sicherheitszonen im Hause identifiziert und angemessen gesichert werden. Zudem muss die EDV-Ausrüstung innerhalb und außerhalb des Hauses angemessen dimensioniert und sicher aufgestellt sein.

5.1. Schutzwürdige Bereiche

Das EGV verfolgt eine Politik des offenen Hauses unter gleichzeitiger Berücksichtigung des Schutzes vertrauenswürdiger und personenbezogener Daten. Diese vermeintlich konträren Ziele bedingen daher eine ausgewogene Berücksichtigung von Offenheit und Sicherheit, sowie entsprechender Praktikabilität und damit zu erreichender Akzeptanz der ergriffenen Maßnahmen.

Zur Erreichung eines Mindestmaßes an Sicherheit sind die folgenden Maßnahmen zu berücksichtigen:

An allen Lokationen, die - aufgrund einer nicht zu erwartenden hohen Besucherfrequenz - über keinen gesonderten Eingangsbereich verfügen, darf der Zutritt nur durch aktives Tun der Mitarbeitenden möglich sein, bspw. durch Anbringen von Klingeln oder Gegensprechanlagen und Begrenzung des Zutritts durch das jeweilige Schließsystem.

Externe Mitarbeiter mit längerfristigen Verträgen können für die Dauer der Verträge eine Zutrittsberechtigung erhalten (z.B. zeitl. begrenzte Zutrittskarten oder Schlüssel für Projektbüros). Voraussetzung hierfür ist die Unterzeichnug einer Geheimhaltungs-/Vertraulichkeits-Vereinbarung und die vertragliche Verpflichtung zur Einhaltung der Informationssicherheits- und Datenschutzregeln des EGV.

Sämtliche Büros, in denen interne Informationen bearbeitet und aufbewahrt werden, müssen abschließbar sein und sollen von den Mitarbeitenden bei Abwesenheit verschlossen werden. Sämtliches Material, welches vertrauliche oder streng vertrauliche Informationen umfasst, ist in separat verschließbaren Schränken aufzubewahren.

In keinem Fall sind vertrauliche Information in allgemein zugänglichen Bereichen offen einsehbar abzulegen.

Als besonders zu schützende Räume gelten im speziellen die Folgenden:

Infrastruktur-Räume sind Räume, die Systeme bzw. System-Komponenten beinhalten, die zum Betrieb der DV-Systeme notwendig sind. Hierzu gehören sowohl die zentralen Netzwerkknoten als auch Anlagen zur Energieversorgung (USV, Stromverteiler, Notstromgeneratoren, ...), Brandmelde- oder Klimaanlagen. Diese Räume sind stets verschlossen zu halten. Die Schlüssel dürfen nur jenen Mitarbeitenden zur Verfügung stehen, die zwingend auf Grund ihrer Tätigkeiten Zutritt und Zugang zu den Infrastruktur-Komponenten benötigen. Die Ausgabe von Schlüssel zu diesen Räumen an Externe über den Empfang, bedarf zwingend der Authorisierung durch den Inneren Dienst und einer Protokollierung.

Dezentrale Netzwerkräume sind Räume, in denen die Etagen- bzw. bereichsübergreifenden Netzwerk-Verkabelungen zusammenlaufen. Diese Räume

sollten ausschließlich die Netzwerkschränke enthalten und auch verschlossen sein. In Ausnahmefällen machen aber bauliche Umstände eine anderweitige Nutzung dieser Räume notwendig. Wenn in diesen Fällen ein Zutritt durch Mitarbeiter notwendig ist, ist dafür Sorge zu tragen, dass die Netzwerkschränke besonders gesichert sind.

Registraturen sind Räume, in denen mehrere Jahrgänge von Akten in Papierform eingelagert sind, die für die Dienst- und Geschäftstätigkeit einer oder mehrerer Organisationseinheiten oder Einrichtungen des EGVs erforderlich sind. Sie müssen mindestens die folgenden Anforderungen erfüllen:

- Eine Brandmeldeanlage ist zu installieren, die zuständige Feuerwehr ist über die Lage und Ausstattung des Raumes zu informieren, damit Löschungen im Notfall nicht mit Wasser durchgeführt werden.
- Grundsätzlich sollte der Zutritt nur einem sehr kleinen, ausgewählten und kontrollierten Personenkreis möglich sein. Die Berechtigung sollte ausschließlich über den Mechanismus einer starken Authentifizierung erfolgen.

Das Rechenzentrum umfasst alle Räume, die für die Dienst- und Geschäftstätigkeit einer oder mehrerer Organisationseinheiten oder Einrichtungen des EGVs erforderliche Server mit Datenbeständen oder Diensten beinhalten. Diese müssen mindestens die folgenden Anforderungen erfüllen:

- Grundsätzlich sind Serverräume in von aussen nicht einsehbaren Räumen unterzubringen. Die Räume dürfen keine wasser- oder dampfführenden Leitungen beinhalten.
- Serverräume sind durch eine feuerbeständige Abtrennung zu den angrenzenden Bereichen, sowie durch entsprechende Türen zu sichern. Kabeldurchbrüche müssen feuerbeständig abgeschottet sein.
- Eine Brandmeldeanlage ist zu installieren.
- Grundsätzlich sollte der Zutritt nur einem sehr kleinen, ausgewählten und kontrollierten Personenkreis möglich sein. Die Berechtigung sollte ausschließlich über den Mechanismus einer starken Authentifizierung erfolgen. Zutritt über einen Schlüssel, der sicher in einem Tresor aufzubewahren ist, darf nur im Notfall erfolgen.
- Unbefugter Zutritt zu Serverräumen sollte überwacht und in entsprechender Weise an die überwachende Instanz gemeldet werden.

5.2. Sicherheit von EDV-Ausstattung

Dezentrale datenhaltende und -verarbeitende EDV-Ausstattung (insbesondere Laptops) muss grundsätzlich unter Aufsicht des verantwortlichen Mitarbeiters sein und darf von diesem nur ausnahmsweise sowie kurz und gesichert unbeaufsichtigt gelassen werden. Mindestens ist der Zugang zu Betriebssystem und Daten zu unterbinden, und die grundsätzliche Aufbewahrung der Ausstattung hat mindestens in geschlossenen Räumlichkeiten zu erfolgen.

Die Aufstellung von EDV-Ausstattung muss dem jeweiligen Schutzbedarf Rechnung tragen, insbesondere sind die Gefahren durch Umwelteinflüsse und Manipulation zu minimieren. Zentrale datenhaltende EDV-Austattung ist nur in Räumen aufzubewahren, die den Anforderungen an das Rechenzentrum (s.o.) genügen.

Unterstützende- und Versorgungseinrichtungen müssen angemessen dimensioniert sein. Die Stromversorgung muss den Anforderungen der betriebenen Ausstattung genügen und bei zentralen Datenbeständen redundant und abgesichert ausgelegt sein (mindestens redundante Stromzufuhr, USVen, Notstromaggregat).

Bei sämtlichen Einrichtungen muss grundsätzlich nach gängigen Standards zur Elektromagnetischen Verträglichkeit vorgegangen werden (DIN EN 61000). Alle relevanten (Bau-)Maßnahmen sind zu dokumentieren. So sind z.B. Datenkabel entsprechend ihrer Funktion zu kennzeichnen, so dass Fehler beim Patchen minimiert werden können.

Bei der Entsorgung oder Wiederverwendung von informationsverarbeitenden Einrichtungen ist darauf zu achten, dass Festplatten mit internen, vertraulichen oder streng vertraulichen Informationen mindestens einmal vollständig überschrieben werden. Bereits defekte Festplatten sind physikalisch zu vernichten.

Die zentrale datenhaltende und informationsverarbeitende und unterstützende Ausstattung muss regelmäßig gemäß den Anforderungen des Herstellers und ggf. von Versicherern gewartet werden. Wartungen und Fehlerbehebungen sind zu protokollieren.

6. Management des Betriebes und der Organisation

Alle Kernverfahren sind zu dokumentieren und unter Informationssicherheits- und Datenschutzgesichtspunkten zu optimieren. Schwerpunkte werden auf Kommunikations-, Datensicherungs- und Netzwerkprozesse gelegt. Basis bildet hier

das Betriebs-Handbuch für das EBK vom jeweiligen für den RZ-Betrieb zuständigen Dienstleister.

Die in den Systemen und Applikationen enthaltenen, für den Dienstbetrieb zentralen Informationen müssen durch Absicherung der Verfahren selbst, durch unterstützende Verfahren und durch organisatorische Regelungen in der eigenen Verantwortung sowie bei den eingebundenen Dienstleistern geschützt werden.

6.1. Verfahren und Verantwortlichkeiten

Die zentralen Verfahren für den Betrieb von DV-Systemen sind zu dokumentieren und umfassen in Abhängigkeit von den konkreten Daten des jeweiligen Systems mindestens die folgenden Punkte:

- Konfiguration der Applikation oder des Servers
- Backup der Daten
- Job-Konfigurationen
- Recovery-Maßnahmen

Die Dokumentationen ermöglichen das Wiederaufsetzen und Wiedereinrichten der Systeme bei Ausfällen und Störungen.

Im Rahmen der Leistungserbringung durch den zentralen DV-Dienstleister geschieht dies in Form des Betriebshandbuches. Handbücher für andere schützenswerte Applikationen und Systeme werden von den Fachadministratoren in Kooperation mit den Dienstleistern geführt. Die Dokumentation anderer intern oder extern erbrachter DV-Dienstleistungen liegt in der Verantwortung der jeweils im EGV für die Leistungserbringung bzw. für die Steuerung des jeweiligen Dienstleisters zuständigen Stelle.

Die Dokumentation ist kontinuierlich auf aktuellem Stand zu halten.

Änderungen an Systemen oder Applikationen, die intern betrieben werden oder intern betriebene Systeme oder Applikationen betreffen (z.B. über Schnittstellen), folgen einem dokumentierten Change-Verfahren (siehe 8.5). Das Verfahren wird in Kooperation durch die Referate Organisation und DV-Service erstellt und aktualisiert und gilt für alle DV-Änderungen im EGV ungeachtet der zuständigen Stelle oder des Dienstleisters.

Für rein extern betriebene Lösungen kann es abweichende Verfahren geben, die aber ebenfalls den hier bestimmten Prinzipien folgen sollen. Konkret betrifft das den

Internet-Auftritt des EGV. Für diesen Bereich gelten die Organisationsverfügung zu Internetdiensten, sowie die Richtlinien zur Internetpräsenz.

Entwicklung-, Test- und Produktivumgebungen sind voneinander physikalisch oder logisch zu trennen. Testverfahren müssen soweit möglich mit anonymisierten oder zumindest pseudonymisierten Daten durchgeführt werden. Die Überführung von Daten und Dateien von Entwicklungs- in Test- und von Test- in Produktivumgebungen (oder umgekehrt) unterliegt dokumentierten Freigabeprozessen.

6.2. Management der Service-Lieferungen von DV-Dienstleistern

Bei der Vergabe von DV-Aufgaben an externe Dienstleister hat die Auswahl des Dienstleisters auch unter Informationssicherheits- und Datenschutzaspekten zu erfolgen. Regelmäßig ist im Rahmen eines Vergabe- und Auslagerungsprojektes eine Bewertung der Auswirkung auf das Sicherheits- und Datenschutzsniveau im EGV durchzuführen. Bei Vertragsabschluss ist zu prüfen, ob gemäß KDO eine Vereinbarung zur Datenverarbeitung im Auftrag zu erstellen ist.

Die relevanten Kennzahlen der Leistungserbringung sind in Service Level Agreements (SLAs) detailliert festzuhalten, die die Ergebnisse der o.g. Bewertung reflektieren.

Alle eingebundenen Dienstleister sind regelmäßig auf die Einhaltung der SLAs hin zu überprüfen. Dazu sind sowohl Performance-Daten der Leistungserbringung durch Überwachung zu berücksichtigen als auch die Auswertung von Berichten des Dienstleisters. Bei Auslagerungsverhältnissen, die Daten der Vertraulichkeitsstufen hoch und sehr hoch beinhalten, sowie bei Auftragsdatenverarbeitung, sind zudem jährlich technische und falls erforderlich organisatorische Auditierungen der Dienstleister durch unabhängige Dritte durchzuführen.

6.3. Systemplanung und Abnahme

Alle internen und externen DV-Ressourcen müssen kontinuierlich im Hinblick auf die Auslastung der Kapazitäten (Festplatten, Netzwerke, CPU,...) überwacht werden. Die jeweils im Fokus der Überwachung stehenden Kapazitäten sind abhängig von der Art der DV-Aufgaben. Die Überwachung kann nach Vorgaben des EGVs auch selbstständig durch den Dienstleister erfolgen, der die Auslastungsdaten monatlich in Berichtform an die verantwortliche Organisationseinheit oder Einrichtung meldet.

Die Abnahme neuer Systeme respektive von Änderungen an Systemen und Applikationen darf nur nach erfolgreicher Durchführung von Testverfahren erfolgen. Die nach Maßgabe des Schutzbedarfs der jeweiligen Systeme durchzuführenden Tests sollen die Funktionalität der Systeme und Applikationen in den konkreten Nutzungskontexten fokussieren. Vor der Freigabe der neuen Versionen müssen konkrete Rollback-Verfahren geplant werden, um im Falle einer nicht erfolgreichen Änderung die alte Konfiguration wieder herstellen zu können.

6.4. Schutz vor Schadsoftware und mobilem Programmcode

Zum Schutz vor Schadsoftware[1] und mobilem Programmcode[2] ist die eigenständige Installation von Software auf den EDV-Anwender-Rechnern technisch zu unterbinden. Serverseitig und auf allen Clients sind Virenscanner installiert, die auch andere Arten von schädlicher Software erkennen können. Die Virendefinitionen werden mindestens täglich aktualisiert. Änderungen an der Engine des Scanners unterliegen dem Change-Verfahren.

Die Verwendung von mobilem Code ist grundsätzlich deaktiviert und wird nur dort dokumentiert zugelassen, wo eine zwingende betriebliche Anforderung nachweisbar besteht.

6.5. Datensicherung

Alle zentralen und dezentralen Datenbestände im gesamten EGV werden mindestens täglich inkrementell und wöchentlich voll gesichert. Die Sicherungsmedien werden dokumentiert und lagern in einem separaten Brandabschnitt getrennt von den gesicherten Datenquellen. Nach jedem Sicherungsvorgang wird die Fehlerfreiheit der Sicherungen geprüft. Mindestens monatlich werden einzelne gesicherte Daten zu Testzwecken wieder eingespielt, um Fehler im Sicherungsprozess erkennen zu können.

6.6. Management von Netzwerksicherheit

[1] Software ist hier im Sinne von in irgendeiner Art auf dem betroffenen System hinterlegten Programmen gemeint.
[2] Mobiler Programmcode meint hier von irgendeiner Quelle ausserhalb des betroffenen Systems nachgeladene („flüchtige"), ausführbare Programme.

Die im EGV zentral und dezentral betriebenen Netzwerke sind ihrem Schutzbedarf entsprechend zu sichern. Systeme und Applikationen mit Daten der Vertraulichkeitsstufen sehr hoch sind soweit möglich in separaten Netzwerksegmenten unterzubringen. Zum Schutz datenhaltender Applikationen sind Firewall-Infrastrukturen zu betreiben, die im Falle von Diensten für die Öffentlichkeit (http, ftp,...) zusätzlich das interne Netz von den öffentlichen Netzteilen abgrenzen.

Eine Erweiterung des potentiellen Nutzerkreises ist nur nach Rücksprache mit der für den Netzbetrieb verantwortlichen Stelle zulässig (bspw. Anschluss eines WLAN-Routers).

Datenübertragung zwischen Netzen im EGV, die über ungesicherte Leitungsabschnitte geht, ist mit geeigneten kryptographischen Verfahren zu verschlüsseln. Der Zugriff auf EGV-Applikationen und -Systeme aus anderen Netzen ist durch ein einheitliches und dokumentiertes Verfahren zu sichern. Das Verfahren muss dem Schutzbedarf der Applikation bzw. des Systems entsprechen.

Netzwerk-Traffic wird kontinuierlich auf Fehler und Unregelmäßigkeiten hin überprüft und protokolliert. Diese Überwachungen dienen ausschließlich der Aufrechterhaltung der Betriebssicherheit und schützen vor unsicheren Inhalten. Personengezogene Auswertungen dürfen gemäß der Dienstvereinbarung IT nur in begründeten Ausnahmefällen vorgenommen werden. Die Details der Auswertung sind separat zu konkretisieren (vgl.6.8) .

Für alle eingesetzten Systeme werden Härtungsrichtlinien entwickelt, die – je nach Maßgabe des Schutzbedarfes bzw. der Verwundbarkeit – die folgenden Punkte abdecken:

- Dokumentation der eingesetzten Netzwerkdienste und deren Erforderlichkeit
- Deaktivierung unsicherer und nicht erforderlicher Dienste
- Sichere Konfiguration erforderlicher Dienste
- Verfahren zur regelmäßigen Überprüfung der Konformität mit der Härtungsrichtlinie

6.7. Austausch von Informationen

Der Austausch von Informationen innerhalb und außerhalb des EGVs muss dem Schutzbedarf der Informationen entsprechend gesichert werden. Beim Austausch von Informationen mit Externen müssen bereits zu Beginn der Zusammenarbeit geeignete Maßnahmen getroffen werden. So müssen alle Externen Verschwiegenheitsvereinbarungen unterzeichnen, wenn sie Zugang zu Informationen der Vertraulichkeitsstufen hoch und sehr hoch erhalten.

Bei geplanter elektronischer Datenübermittlung sind zudem die Übertragungswege geeignet zu sichern. Bei einer auf Dauer angelegten kontinuierlichen Kommunikation von Informationen der Vertraulichkeitsstufen hoch und sehr hoch, ist eine Verschlüsselung der Übertragungswege einzurichten. Bei fallweiser Kommunikation von Informationen der Vertraulichkeitsstufen hoch und sehr hoch z.B. über Emails, sind Werkzeuge zur Verschlüsselung von Dateien zur Verfügung zu stellen.

Bei der Übermittlung von Informationen sind auch die Schnittstellen zwischen Applikationen in Hinblick auf Sicherheitsschwachstellen zu beachten.

Der Transport von Informationen der Vertraulichkeitsstufen hoch und sehr hoch auf Datenträgern (dies beinhaltet CDs, DVDs, USB-Sticks, externe Festplatten und Notebook-Festplatten, sowie alle anderen mobilen Speicher) darf nur verschlüsselt erfolgen. Zudem müssen sich die Datenträger während des Transportes konstant in der Obhut der zuständigen Person befinden. Die Aufbewahrung dieser Datenträger darf nur unter Verschluss erfolgen.

6.8. Überwachung und Monitoring

Der lesende und schreibende Zugriff auf personenbezogene Daten und Informationen der Vertraulichkeitsstufen hoch und sehr hoch in Applikationen des EGVs ist kontinuierlich zu protokollieren.

Gegenstand des Protokolls ist in der Regel mindestens:

- Benutzerkennung,
- Uhrzeit,
- Zugriffsversuche,
- Änderungen an Daten
- Ausgelöste Alarme,
- Fehler.

Hiervon abweichende oder darüber hinausfgehende Protokolldaten sind in den jeweiligen Fachverfahren dokumentiert. Besondere Beachtung verdient auf Grund des hohen Missbrauchpotentials die Protokollierung von Administratorentätigkeiten.

Wenn in den Fachverfahren keine anderen Vorgaben gemacht werden, sind die Protokolldaten für eine Dauer von mindestens vier Wochen separat aufzubewahren und entsprechend zu sichern.

Alle Systeme im Netz des EGVs müssen über einen zentralen oder mehrere gleichlaufende Zeitserver synchronisiert werden, um die chronologische Auswertung von Ereignissen zu ermöglichen.

Die Protokolldaten werden kontinuierlich durch geeignete Monitoring-Werkzeuge überwacht, die bei Über- oder Unterschreitung definierter Grenzwerte die zuständigen Administratoren alarmieren.

7. Sicherheit der Zugänge

Das Management der Zugänge zu den Netzwerken, Applikationen und Systemen ist so zu gestalten, dass Dienst- und Informationssicherheitsanforderungen vereint und die unterschiedlichen Modalitäten des Arbeitens in Betracht gezogen werden (mobile Arbeit, Telearbeit,...). Die Verantwortung der Anwender für die Sicherheit der Zugänge ist zu stärken.

7.1. Verwaltung der Anwender

Der Zugang zu den Netzwerken, Systemen und Applikationen im EGV unterliegt einem Anwenderregistrierungsprozess, der für die zentralen Systeme über die DV-Beauftragten erfolgt. Die dezentralen Systeme sind in der Verantwortung der zuständigen Organisationseinheit oder Einrichtung zu verwalten.

Alle Anwender erhalten eindeutige Kennungen, Sammelaccounts sind grundsätzlich nicht zulässig. Ausnahmen gelten nur für lesenden Zugriff auf nicht-personenbezogene oder personenbeziehbare Datenbestände der Vertraulichkeitsstufen öffentlich oder intern. Alle Anwenderrechte auf Netzwerken, Systemen und Applikationen müssen dokumentiert werden.

Rechte sind nur auf Basis des Erforderlichkeitsgrundsatzes (Need-to-Use) zu verteilen. Dies gilt insbesondere für Sonderrechte (Administrator, Operator,...). Für den Zugang zu Netzwerken, Systemen und Applikationen sind initiale Passwörter zu vergeben, die bei der ersten Anmeldung durch den Anwender zu ändern sind (pre-expired). Passwörter müssen mindestens acht Zeichen haben und hohe Komplexitätsanforderungen erfüllen. Die Verwendung der letzten fünf Passwörter ist nicht zulässig. Eine Änderung der Passwörter erfolgt spätestens alle drei Monate und höchstens alle 48 Stunden. Passwörter sind strikt geheim zu halten.

Halbjährlich überprüfen die für den Betrieb Verantwortlichen (d.h. Fach- und Systemadministratoren) stichprobenhaft die Benutzerberechtigungen, um Rechte aufzudecken, die nicht dem Erforderlichkeitsgrundsatz entsprechen. Die Änderung von Benutzerrechten unterliegt einem Change-Management.

7.2. Verantwortung der EDV-Anwender

EDV-Anwender sind angewiesen, bei der Verwendung von Passwörtern auf die Geheimhaltung und Qualität der Passwörter zu achten. Zudem muss die eingesetzte Hardware vor Verlust und Missbrauch geschützt werden. Dazu sind insbesondere Sitzungen bei Verlassen des Arbeitsplatzes zu sperren, bzw. nach Ende der Tätigkeiten Abmeldungen von Servern durchzuführen. Informationen mit hohem oder sehr hohem Schutzbedarf dürfen nicht unverschlossen in Büros zurück gelassen werden.

7.3. Zugang zu Netzwerken

Die Konfiguration von Netzwerken und die Maßnahmen zur Sicherung der Netzwerke sind jeweils zu dokumentieren. Insbesondere ist zu beachten, dass ein Remote-Zugang zu zentralen Systemen und Applikationen im EGV grundsätzlich nur über entsprechend gesicherte Verbindungen möglich sein darf. In der Regel sind das VPN-Verbindungen. Bei Zugang auf zentrale Datenbestände über Webschnittstellen ist die Absicherung durch SSL erforderlich. Webschnittstellen sind zudem auf technische Schwachstellen zu überprüfen (Session Management und Authentication). Bei der Konfiguration der Netzwerke sind die Diagnoseports sicher zu konfigurieren bzw. zu schützen.

Die Verwendung fremder Geräte im Netz des EGVs muss durch geeignete technische Maßnahmen überall dort unterbunden werden, wo dies nicht zwingend erforderlich ist (z.B. in Konferenzräumen).

Netzwerke sind unter Sicherheitsgesichtspunkten zu segmentieren. Datenbestände der Vertraulichkeitsstufe sehr hoch können in eigenen VLANs oder sogar als Insellösung betrieben werden.

Verbindungen zu den Netzwerken des EGVs werden kontinuierlich überwacht. Die zulässigen Verbindungen zu den eingerichteten Diensten werden technisch gesteuert und unterliegen zeitlichen Beschränkungen (Timeout, maximale Verbindungszeit).

Die Routing-Konfigurationen in den Netzwerken werden lückenlos dokumentiert.

Bei der Verwendung von WLAN durch Organisationseinheiten oder Einrichtungen des EGVs ist auf eine angemessene Verschlüsselung wert zu legen. Eine Verschlüsselung mit WEP wird nicht als ausreichend betrachtet. Der Einsatz von WLAN-Technologie in Netzen des EGVs sowie der Anschluss externer Netze an EGV-Netze setzt die Freigabe der für den Netzbetrieb verantwortlichen Stelle voraus.

7.4. Zugang zu Betriebssystemen

Die Anmeldung an Betriebssystemen im Netz des EGVs ist durch ein sicheres Anmeldeverfahren geschützt, wobei die Anzahl erfolgloser Anmeldeversuche auf fünf begrenzt ist. Nach drei Fehleingaben wird eine zeitlich befristete Sperre für den entsprechenden Account eingerichtet. Eine Entsperrung erfolgt nur über den 1.-Level-Support.

Alle Nutzer erhalten eindeutige Benutzerkennungen, Sammelaccounts sind nicht zulässig. Die einzige Ausnahme bilden hier die systemseitig notwendigen Administrator-Accounts, deren Passworte nur den namentlich genannten Systemadministratoren bekannt ist. Zur Authentisierung der Nutzer werden geeignete Authentisierungstechniken eingesetzt, d.h. im Haus Benutzername und Passwort, außerhalb des Hauses Benutzername, Passwort und ein weiteres Authentifizierungsmerkmal (z.B. ein digitales Zertifikat, welches auf dem System installiert ist).

Soweit möglich werden die Möglichkeiten von Systemen zur Unterstützung bei der Generierung qualitativ hochwertiger Passwörter genutzt.

Die Verwendung von Systemwerkzeugen (i.d.R. zur Verwaltung und Konfiguration) ist auf Administratoren zu beschränken. Grundsätzlich schließt dies Fachadministratoren nicht mit ein.

7.5. Zugang zu Applikationen

Nutzer im EGV dürfen mit ihren individuellen Zugriffs- und Zugangsrechten nur solche Daten lesen und schreiben, die sie aufgrund ihrer Aufgaben lesen oder schreiben müssen. Ein Zugang zu Applikationen – lesend oder schreibend – mit personenbezogenen, vertraulichen oder streng vertraulichen Daten ohne konkrete Bindung an eine Aufgabe des Mitarbeitenden ist nicht zulässig. Die Rechteverwaltung folgt einem strikten Erforderlichkeitsprinzip (Need-to-Know).

Ggf. sind unter Berücksichtigung der Sicherheitsanforderungen besondere Maßnahmen oder sogar Einschränkungen notwendig, wenn z.B. Telearbeit oder mobiles Equipment zum Einsatz kommen soll. Diese sind gesondert festzulegen.

Zum Einsatz kommen im EGV ausschließlich Anwendungen, die in Bezug auf Funktionalität und Sicherheit abgenommen sind und damit dem internen Standard entsprechen. Installationen erfolgen ausschließlich durch das Referat DV-Service oder den autorisierten Dienstleister nach dem geregelten Change-Verfahren.

8. Sicherheit in Beschaffung, Entwicklung und Wartung

Um frühzeitig ein einheitliches und angemessenes Informationssicherheits- und Datenschutzniveau anzustreben sind Sicherheitsanforderungen insbesondere in den Beschaffungs-, Wartungs- und Entwicklungsprozessen des EGVs zu berücksichtigen. Einen wesentlichen Schwerpunkt bildet dabei die Vereinheitlichung und Optimierung von Eigenentwicklungen unter Informationssicherheits- und Datenschutzaspekten.

8.1. Sicherheitsanforderungen bei Beschaffungsverfahren

Bei der regelmäßigen Beschaffung von EDV-Ausstattung müssen Sicherheitsanforderungen, die sich aus dem Schutzbedarf der Ausstattung und aus ihrem Verwendungszweck ergeben, berücksichtigt werden. Bei großangelegten EDV-Projekten mit dem Ziel der Einführung neuer Systeme und Applikationen ist der ZISB im Vorfeld einzubeziehen, um das Vorhaben unter Sicherheitsgesichtspunkten zu bewerten.

Bei der Beschaffung sicherheitsrelevanter Ausstattung über die Abteilung Innerer Dienst ist der ZISB ebenfalls einzubeziehen.

Zur Erreichung dieser Ziele ist ein einheitliches Beschaffungsverfahren zur Verwendung durch alle Organisationseinheiten und Einrichtungen unter Berücksichtigung eines entsprechenden Meilensteins zu definieren.

8.2. Sichere Datenverarbeitung und Entwicklung

Bei der Entwicklung neuer und der Fortentwicklung bestehender zentraler datenhaltender Applikationen mit Daten der Vertraulichkeitsstufen „hoch“ oder „sehr hoch“ oder hohen bis sehr hohen Anforderungen an die Integrität der Daten sind Plausibilitäts- und Integritätsprüfungen zu implementieren. Gleiches gilt für dezentrale Anwendungen, die für die Aufrechterhaltung der Dienst- und Geschäftstätigkeit einer Organisationseinheit oder Einrichtung erforderlich sind. Auf diesem Wege ist sicherzustellen, dass Eingabe- und Ausgabedaten korrekt und gültig sind, und dass bei der Verarbeitung und Übertragung von Daten die Integrität und Vertraulichkeit der Daten gewahrt bleibt.

Des Weiteren sind für die Entwicklung von hauseigenen Datenbanken und Datenbankapplikationen systematische Entwicklungsstandards zu erstellen und zu Grunde zu legen. Das Vorgehen muss Sicherheitsgesichtspunkte berücksichtigen.

Bei der Entwicklung von webbasierten Applikationen für die Öffentlichkeit ist das Vorgehen nach OWASP (Open Web Application Security Project) zu Grunde zu legen.

Vor der Umsetzung jedes Projektes zur Verarbeitung von Daten ist unabhängig davon, ob das Projekt ein technisches oder prozessorientiertes Ziel verfolgt, eine Risikobewertung durchzuführen, deren Ergebnisse sich in konkreter Weise in Maßnahmen bei der Implementierung wiederfinden. Insbesondere sind die gängigsten Schwachstellen zu überprüfen und das Ergebnis der Überprüfung zu dokumentieren. Abweichungen von den o.g. Standards können in Einzelfällen statthaft sein, wenn die Risikoanalyse entsprechend geringe Gefahren ausweist und besondere (z.B. ökonomische) Gründe dafür sprechen.

Die Einhaltung der Sicherheitsanforderungen wird jährlich im Auftrag des ZISB überprüft.

8.3. Einsatz von Verschlüsselungstechnologien

Für die Verschlüsselung und verschlüsselte Übertragung von Informationen der Vertraulichkeitsstufen hoch und sehr hoch zu vertrauenswürdigen externen Partnern werden angemessene Technologien zur Verfügung gestellt. Vorzugsweise werden asymmetrische Schlüssel-Infrastrukturen aufgebaut. Die Verschlüsselung muss nach gängigen Sicherheitsstandards in Kombination mit Schlüsseln einer Mindest -Länge und –Komplexität erfolgen, die nach jeweiligem Stand der Technik als sicher gelten. Bei Informationen der Vertraulichkeitsstufe „hoch“ ist die verschlüsselte Übertragung zwischen Servern zulässig, bei Informationen der Vertraulichkeitsstufe „sehr hoch“ müssen Dateien und Informationsträger einzeln verschlüsselt werden.

8.4. Sicherheit von System- und Testdaten

Sowohl extern eingekaufte als auch eigenentwickelte installierte Software muss gesichert verwahrt werden, so dass ein späterer Zugriff für Administratoren jederzeit möglich ist. Bei selbstentwickelter Software sowie bei eingekauften Entwicklungstätigkeiten sind die Quelltexte angemessen zu sichern und zu dokumentieren.

Die im Rahmen von Testverfahren genutzten Systeme müssen den gleichen Sicherheitsanforderungen genügen wie die Systeme für den operativen Betrieb, wenn personenbezogene, vertrauliche oder streng vertrauliche Daten verarbeitet werden. Alternativ können Verfahren der Anonymisierung und Pseudonymisierung eingesetzt werden, um den Schutzbedarf der Testdaten zu senken.

8.5. Change-Management

Um die Sicherheit betriebener Systeme zu gewährleisten und den Betrieb zu kontrollieren, sind die Vorgaben des zentralen Change-Management-Prozesses in der jeweils aktuellen Fassung einzuhalten. Der Change-Management-Prozess gilt für sämtliche Systeme und Applikationen unabhängig von den an der Leistungserbringung beteiligten Stellen.

Bei der Gestaltung von Wartungs- und Change-Management-Verfahren wird das Vier-Augen-Prinzip verwirklicht. Die Freigabe für eine Änderung und deren Umsetzung ist zwei getrennten Rollen zugewiesen. In der Praxis findet sich diese Aufgabenteilung in der Regel in Form der Trennung zwischen fachlich verantwortlichem Mitarbeitenden und Dienstleister wieder. Zur Wahrung der informationsicherheitstechnischen Aspekte ist grundsätzlich der ZISB in das Change-Verfahren einzubinden. Diese Einbindung erfolgt informell (bei kleineren Änderungen) bzw. freigebend bei größeren Änderungen (sicherheitsrelevante Änderungen, Projekte, neue Software, ...); Standard-Changes erfolgen ohne Einbindung des ZISB.

Nach jeder durchgeführten Änderung an Betriebssystemen sind die betriebenen Applikationen technisch auf Schwachstellen hin zu überprüfen.

8.6. Management von Schwachstellen

Informationen über technische Schwachstellen sind kontinuierlich vom jeweiligen Hersteller zu beziehen und von den Fach- sowie DV-Administratoren zu bewerten. Geeignete Maßnahmen sind von den Fach- und DV-Administratoren zu planen und koordiniert im Rahmen des Change-Managements durchzuführen.

9. Management von Informationssicherheitsvorfällen

Der Umgang mit Sicherheitsvorfällen muss sowohl das Erkennen und Behandeln von Risiken, als auch die Nachhaltung und Überprüfung korrektiver Maßnahmen berücksichtigen. Neben der technischen Überwachung unserer Systeme sind auch die Mitarbeitenden eine wichtige Quelle für Meldungen von Sicherheitsvorfällen und müssen entsprechend sensibilisiert werden. Wichtig sind neben der unmittelbaren Reaktion auf Vorfälle auch die aus Vorfällen resultierende Optimierung unseres Sicherheitsmanagements und die Überwachung von Maßnahmen auf dauerhafte Wirksamkeit. Aus Fehlern soll systematisch gelernt werden.

9.1. Meldung von Sicherheitsvorfällen und Schwachstellen

Ein Vorfall ist jede Abweichung vom normalen Betrieb unserer Applikationen und Systeme. Als Sicherheitsvorfälle gelten dabei jedoch nur solche Ereignisse, die unmittelbar oder mittelbar auf die Schutzziele und die Sicherheit unserer Datenbestände wirken. Sicherheitsrelevante Vorfälle können sämtliche Schutzziele von der Verfügbarkeit, über die Vertraulichkeit bis zur Verlässlichkeit (Integrität/Authentizität) betreffen. Folgende Beispiele verdeutlichen das:

Ausfall von Endgeräten	Verf.
Ausfall von Server-Systemen und zentralen Netzkomponenten	Verf.
Verlust eines Zugangsschlüssels oder der Zugangskarte	Vertr.
Verlust von Hardware mit Daten	Vertr.
Missbrauch von Systemen	Vertr.
Unbefugte Weitergabe von Daten	Vertr.
Fehler in datenverarbeitenden Systemen aufgrund von Fehleingaben	Verl.
Fehler in datenverarbeitenden Systemen aufgrund technischer Ursachen	Verl.
Passwort-Missbrauch	Vertr., Verl.
Befall mit Viren oder Malware	Verf., Vertr., Verl.

Zur Lösung von sicherheitsrelevanten Vorfällen ist die unmittelbare Einbindung des ZISB nicht zwingend notwendig. Es besteht aber eine generelle Informationspflicht an den ZISB. Da in Abhängigkeit von der Dringlichkeit und den (mögl.) Auswirkungen

ein Eingreifen des ZISB erforderlich sein kann, hat die Information an den ZISB unverzüglich nach der Erfassung der Vorfälle zu erfolgen.

Mitarbeitende sind zudem aufgefordert, Schwachstellen in Applikationen und Systemen zu melden, sofern sie bei der Benutzung zutage treten. Schwachstellen können sein:

- Wenn EDV-Anwender weiterreichende Funktionen außerhalb ihres Aufgabenbereiches ausüben können, obwohl sie dafür nicht autorisiert sind.
- Wenn Applikationen und Systeme ungewöhnliches Verhalten zeigen.
- Wenn Unbefugte über Sicherheitslücken Zugriff auf Informationen und Datenbestände haben könnten.

Die Meldung sämtlicher Vorfälle und Schwachstellen erfolgt über das Ticket-System der verantwortlichen Stelle. Nach Aufnahme der sicherheitsrelevanten Tickets sowie nach Abschluss der Bearbeitung werden unmittelbar der ZISB sowie das Referat DV-Service beziehungsweise die für den Betrieb verantwortliche Stelle informiert.

9.2. Management von Sicherheitsvorfällen und Lernen aus Fehlern

Primäres Ziel ist die zeitnahe Wiederherstellung der betroffenen Systeme. Unter diesem Aspekt sind für die oben definierten sowie alle weiteren erkannten, sicherheitsrelevanten Vorfälle entsprechende Verantwortlichkeiten und Verfahren zu definieren.

Zusätzliches Ziel ist die Verhinderung weiterer Kompromittierung oder Infizierung von Systemen und Applikationen. Es ist daher erforderlich, die relevanten Vorfälle in der Kontinuitäts-Planung und in den Wiederanlaufplänen der Systeme zu berücksichtigen.

Zusätzlich zu der Meldung durch Mitarbeitende werden die zentralen Applikationen und Systeme kontinuierlich vom Dienstleister durch ein Monitoring-Tool überwacht. Vom System generierte Meldungen werden an die verantwortlichen Administratoren gemeldet.

Die Sicherheitsvorfälle sollen monatlich aggregiert dem ZISB zur Verfügung gestellt werden, so dass dieser die Arten und Häufigkeit der Vorfälle auswerten und Trends frühzeitig erkennen kann.

Alle korrektiven Maßnahmen sollen in einem angemessenen Zeitraum nach der Implementierung überwacht und auf ihre Wirksamkeit überprüft werden.

Manche Vorfälle können zivil- oder strafrechtliche Relevanz besitzen, wie beispielsweise:

- Missbrauch des EGV-Netzwerkes für Attacken auf andere Netzwerke oder Rechner
- Missbrauch von EGV-Systemen als Download-Server für urheberrechtlich geschützte Materialien
- Missbrauch von EGV-Systemen zum Zugriff auf illegale Medienangebote
- Unbefugtes Eindringen in EGV-Systeme
- Kompromittierung von EGV-Datenbeständen

In diesen Fällen sind vom Dienstleister die folgenden Beweissicherungsverfahren durchzuführen:

- Sicherung sämtlicher Protokolle der betroffenen Systeme
- Erstellung von Speicherdumps unmittelbar kompromittierter Systeme
- Erstellung von Festplattenimages unmittelbar kompromittierter Systeme
- Erstellung eines Prüfwertes der gesicherten Daten

10. Kontinuierliche Fortführung des Dienst- und Geschäftsbetriebes

Auch im Falle des Eintretens eines Bedrohungsszenarios müssen die erforderlichen DV-Leistungen zur kontinuierlichen Aufrechterhaltung des Dienst- und Geschäftsbetriebs zur Verfügung stehen. Die Notfallmaßnahmen, die Priorität von Systemen und Applikationen untereinander und die Mindestanforderungen an deren Betrieb müssen unter Berücksichtigung der jeweiligen Anforderungen an den Schutzbedarf von Systemen, Applikationen und Informationen geplant werden.

10.1. Risikobewertung für den Dienst- und Geschäftsbetrieb

In Kooperation mit dem Referat DV-Service und den für dezentralen Betrieb von IT-Dienstleistungen verantwortlichen Stellen führt der ZISB jährlich eine Risikobewertung auf Basis der aktuellen Schutzbedarfsfeststellungen durch. Dem ZISB obliegt die Wahl der Methodik, die zu einer Bewertung der Risiken anhand von Bedrohungsszenarien (z.B. Ausfall von Geräten, menschliche Fehler, Diebstahl, Feuer, Naturkatastrophen und Terrorakte) sowie deren Eintrittswahrscheinlichkeit und Auswirkungen führt.

Die Analyse hat die Identifizierung, Quantifizierung und Priorisierung von Risiken zum Ziel und dient der Identifikation kritischer Ressourcen, von Auswirkungen von Unterbrechungen, zulässiger Ausfallzeiten und Wiederherstellungsprioritäten.

10.2. Entwicklung und Umsetzung von Notfallplänen

Auf Basis der Ergebnisse der jährlichen Risikobewertung werden Pläne entwickelt und umgesetzt, um den Betrieb im Notfall aufrechtzuerhalten oder wieder herzustellen, und um die Verfügbarkeit zwingend notwendiger Informationen in dem erforderlichen Zeitraum nach Unterbrechungen oder Ausfällen von kritischen DV-Dienstleistungen sicherzustellen.

Der Planungsprozess umfasst die folgenden Punkte:

- Identifizierung und Vereinbarung der Verantwortlichkeiten, sowie
- Identifizierung des akzeptablen Verlusts von Informationen und Services
- Umsetzung von Verfahren um eine Wiederherstellung des Dienst- und Geschäftsbetriebs und der Verfügbarkeit von Informationen in Kooperation mit den DV-Dienstleistern innerhalb des geforderten Zeitrahmens zu ermöglichen
- Dokumentation vereinbarter Verfahren und Prozesse
- angemessene Ausbildung für Mitarbeitende in den vereinbarten Verfahren und Prozessen (in Zusammenarbeit mit der „Personalentwicklung")
- Testen und Aktualisierung der Notfall-Pläne

Notfall-Pläne behandeln die Schwachstellen des EGVs und enthalten daher Informationen der Vertraulichkeitsstufen hoch und sehr hoch, die entsprechend geschützt werden müssen. Kopien der Notfall-Pläne werden an einem entfernten Ort gespeichert, um Schäden durch Katastrophen am Hauptstandort zu entgehen.

Durch regelmäßige Tests der Notfall-Pläne wird sichergestellt, dass sich alle Mitarbeitenden in der Administration und andere relevante Mitarbeitenden, die zur Wiederherstellung der System-Funktionalität benötigt werden, der Pläne und ihrer Verantwortung bewusst sind, und dass sie ihre Rolle kennen, wenn ein Plan aktiviert wird.

11. Datenschutz und Konformität

Essentiell für das Informationssicherheits- und Datenschutzmanagement im EGV sind die Vorgaben aus der KDO. Diese Vorgaben gelten auch für alle angeschlossenen Einrichtungen sowie sonstige Partner im Sinne des Geltungsbereiches, die sich hierauf zu verpflichten haben.

11.1. Organisation des Datenschutzes

Die Überwachung der Einhaltung von Datenschutzanforderungen obliegt in allen eigenständigen Organisationeinheiten des EBKs und damit auch im EGV den betrieblichen Datenschutzbeauftragten. Datenschutzbeauftragte sind weiterhin von allen Dienstleistern zu bestellen, die im Rahmen von Auftragsdatenverarbeitungsverhältnissen personenbezogene Daten für die Einrichtungen und Organisationseinheiten des EGVs verarbeiten. Hier sind mit diesen Dienstleistern entsprechende Vereinbarungen gemäß §8 der KDO zu treffen.

Zur Erarbeitung und Umsetzung konkreter Maßnahmen ist eine enge Zusammenarbeit mit dem ZISB vorgesehen.

Der Diözesandatenschutzbeauftragten obliegen als Kontrollinstanz die folgenden Aufgaben:

- Überwachung der Einhaltung der KDO
- Empfehlung von Maßnahmen
- Beratung der bischöflichen Behörde und sonstiger Dienststellen
- Erstellung von Gutachten und Berichten

11.2. Aufgaben der betrieblichen Datenschutzbeauftragten

Die Aufgaben der betrieblichen Datenschutzbeauftragten umfassen gemäß §18a, b der KDO u.a.:

- Hinwirken auf die Einhaltung der Vorschriften der KDO im kirchlichen Betrieb
- Überwachung des ordnungsgemäßen DV-Einsatz
- Sensibilisierung der Mitarbeitenden zu den Anforderungen der KDO
- Bearbeitung von Anfragen
- Führen des Verfahrensverzeichnisses

11.3. Überwachung gesetzlicher Vorgaben in betrieblichen Abläufen

In enger Kooperation mit dem ZISB sind die leitenden Mitarbeitenden zur Identifikation, Umsetzung und Einhaltung einschlägiger handels-, steuer- und wettbewerbsrechtlicher Vorgaben sowie regulatorischer Anforderungen und der Maßnahmen aus dieser Richtlinie in ihren Zuständigkeitsbereichen aufgefordert.

Direktor HA-Verwaltung

Köln; Datum: 14.05.14

Anlage 1 - Rollen/Funktionen

Anwender

Alle Personen, die in irgendeiner Weise DV- Dienstleistungen des EGV in Anspruch nehmen. Neben allen Beschäftigten des EGV sind das auch Mitarbeitende der Rendanturen, oder anderer Institutionen und kirchlicher Einrichtungen bis hin zu Externen, die in irgendeiner Form (temporär) im oder für das EGV tätig sind.

DV-Beauftragte

Jeder Fachbereich bestimmt für seine Anwender einen DV- Beauftragten. Die DV-Beauftragten fungieren als erster Ansprechpartner für die Anwender, wenn es um inhaltliche oder funktionale Fragen zu fachspezifischen Anwendungen geht. Insbesondere sind sie auch erster Ansprechpartner, wenn es um "Wünsche" oder "Anforderungen" geht, die z.B. Ausstattung, Berechtigungen, oder zusätzliche Funktionen betreffen. Umgekehrt sind sie auch erste Ansprechpartner des Referates DV-Service und fungieren quasi als Multiplikatoren für die Fachbereiche.

Servicedesk

Im Servicedesk werden sämtliche Anforderungen aufgenommen, die insbesondere Fehler, Störungen oder andere benötige Unterstützungs-Leistungen (Supportanfragen) betreffen.

Soweit wie möglich werden diese Vorfälle vom 1.-Level- Support bearbeitet und gelöst.

Können die Vorfälle vom 1.-Level-Support nicht in einem kurzen Zeitrahmen gelöst werden, wird der 2.-Level-Support eingebunden.

1.-Level-Support

In der Regel die direkten Mitarbeitenden im Service- Desk.

Der Service-Desk wird im EGV vom zentralen IT- Dienstleister besetzt.

2.-Level-Support

Fachleute zu speziellen Themen, die vom Service- Desk hinzugezogen werden, hierzu gehören in erster Linie die Fach- und System- Administratoren.

Administration

Fachadministration
Administratoren mit speziellen Kenntnissen und Berechtigungen zu einer bestimmten Fachanwendung.

I.d.R. sind die Fachadministratoren im Bereich DV-Service angesiedelt. Ausnahmen sind hier möglich, wenn die notwendigen Kenntnisse sehr fach- oder gar hersteller-spezifisch sind. Dann kann diese Rolle in einem Fachbereich oder bei einem externen Dienstleister angesiedelt sein.

Systemadministration
Die hardware- und betriebssystemnahe Administration liegt bei unserem zentralen IT- Dienstleister, der für den Betrieb des Rechenzentrums zuständig ist.

ZISB
Zentraler Informations- Sicherheitsbeauftragter

Im EGV die zuständige Instanz für alle Themen, die sich um Informations- und Datensicherheit drehen.

Sicherheits-Team
Zur Lösung spezifischer, sicherheitsrelevanter Aufgaben, wird vom ZISB ein passendes Sicherheits-Team aus entsprechenden Experten zusammen gestellt. I.d.R. werden hier Vertreter aus "Zentrale Dienste" und/oder die Datenschutzbeauftragten tätig; aber auch Mitarbeitende aus einzelnen Fachbereichen oder externe Spezialisten können hinzu gezogen werden.

Bei den Themen, die den zentralen IT-Dienstleister betreffen, entspricht das Sicherheits-Team quasi dem Security-Board.

Security-Board
Im Security-Board werden alle sicherheitsrelevanten Themen behandelt, in die der zentrale IT-Dienstleister involviert ist.

Das Security-Board besteht aus den Informations- Sicherheits-Beauftragten des EGV und des zentralen IT- Dienstleisters. Hinzu kommen - in Abhängigkeit von den zu behandelnden Themen - entsprechende Experten.

Datenschutz

Der Datenschutz umfasst und beschreibt die speziellen Anforderungen an die Informations- und Datensicherheit, wenn es sich um personenbezogene Daten handelt.

dDSB
Diözesan- Datenschutzbeauftragte/r

Bistumsübergreifende Instanz mit beratender und kontrollierender Funktion

bDSB
Betriebliche/r Datenschutzbeauftragte/r

zuständig für die Umsetzung und Einhaltung der Datenschutz-Vorschriften im EGV und Ansprechpartner/Bearbeiter bei allen Anfragen an das EGV, die den Datenschutz betreffen.