EDV-Ordnung des Bistums Mainz

vom 21. Mai 2002

(Kirchliches Amtsblatt für die Diözese Mainz 2002, Nr. 6, Ziff. 81, S. 37 ff.)

1. Allgemeines

1.1 Ziele und Geltungsbereich

Diese Ordnung regelt die Rechte und Pflichten des Dienstgebers und aller Mitarbeiter[1], die an der Vernetzung teilnehmen, im Zusammenhang mit der direkten oder indirekten Nutzung sowie der Pflege, Wartung und Weiterentwicklung der in dieser Ordnung genannten EDV-Anlagen. Mitarbeiter i.S. dieser Ordnung sind auch nebenamtliche und ehrenamtliche Mitarbeiter, Praktikanten etc.

Diese Ordnung bezieht sich auf den Einsatz aller Anlagen zur elektronischen Datenverarbeitung im Bischöflichen Ordinariat, die mit Hilfe des Netzwerkes, das vom Bischöflichen Ordinariat betrieben wird, zusammengeschlossen sind. Sie gilt auch für den Einsatz des angebundenen Großrechners.

Diese sind im Folgenden als EDV-Anlagen bezeichnet.

Die Ordnung regelt ferner die Zulassung zu Kommunikationsdiensten, die innerhalb der Vernetzung bereitgestellt werden und auf die von externen Nutzern zugegriffen werden kann. Dies gilt jedoch nicht für den Bereich der Telefonie und des Faxversands soweit letzterer nicht von EDV-Systemen durchgeführt wird

1.2 Datenschutz

Jeder Mitarbeiter ist verpflichtet, beim Umgang mit personenbezogenen Daten das Persönlichkeitsrecht des Einzelnen zu schützen. Die Anordnungen über den kirchlichen Datenschutz und die hierzu ergangenen Ausführungsbestimmungen sind in ihrer jeweiligen Fassung zu beachten. Zur Zeit gilt die Anordnung über den kirchlichen Datenschutz – KDO – gem. Amtsblatt 1994 Seite 13. Zweifelsfälle sind über den Generalvikar dem Datenschutzbeauftragten des Bistums vorzutragen.

---

1 Wegen der einfacheren Lesbarkeit des Textes wird nach Absprache im Lenkungsausschuss die männliche Form im Text verwendet.

2. Begriffsbestimmungen

2.1 Zugang/Zugangsberechtigung

Für den Zugang ist eine Zugangsberechtigung notwendig. Diese ist die Kombination aus einem vorgegebenen Benutzernamen und einem geheimen Kennwort (s. auch Ziff. 6.2). Benutzername und Kennwort sind notwendig, um Zugang zu den EDV-Anlagen zu erhalten.

2.2 Zugriff

Zugriff ist die Möglichkeit, bestimmte Verzeichnisse und Dateien oder andere Ressourcen zu öffnen oder zu verwenden.

2.3 Software

Software sind Programme zur Ausführung auf den Computern der EDV-Anlagen.

2.4 Organisationseinheit

Eigenständige Organisationseinheiten sind in der Anlage genannt.

2.5 Elektronische Kommunikation

Im Sinne der Verordnung ist elektronische Kommunikation die mit Hilfe von Computern bewusst durchgeführte oder versuchte Informationsübermittlung zwischen mindestens zwei Personen. Beispiele sind die Übermittlung elektronischer Nachrichten (E-Mail) oder Video- und Audioübertragungen.

3. Zugangsberechtigung

Der zuständige Vorgesetzte (z.B. Abteilungsleiter, Regens) und der zuständige Dezernent entscheiden über die Erteilung einer Zugangsberechtigung. Sie leiten den Antrag an die Administratoren in der EDV-Abteilung (im weiteren Text „Administratoren“ genannt) weiter. Die Administratoren bearbeiten und bewahren die Anträge auf Zugangsberechtigung auf. Gleichzeitig gibt der Mitarbeiter eine Verpflichtungserklärung ab, in der er sich verpflichtet, diese Ordnung sorgfältig einzuhalten und die damit zusammenhängende Dienstvereinbarung zu beachten. Er bestätigt dabei, über die Anforderungen des Datenschutzes unterrichtet zu sein. Zugangsberechtigungs- und Verpflichtungserklärungsformular sind in der Anlage zu dieser Ordnung enthalten.

Zugangsberechtigungen werden nur natürlichen Personen erteilt.

Die Einrichtung einer Zugangsberechtigung kann zeitlich befristet werden. Bei einer Befristung sperren die Administratoren die Zugangsberechtigung automatisch zum Ende des genehmigten Zeitraums.

Die Administratoren weisen dem Anwender bei Einrichtung einer Zugangsberechtigung einen individuellen Benutzernamen und ein anfängliches Kennwort zu. Die Administratoren wählen die Benutzernamen nach technischen Kriterien. Ein Recht auf die Zuweisung eines bestimmten Benutzernamens besteht nicht.

Der Anwender ist verpflichtet, das anfänglich zugewiesene Kennwort sofort nach Erhalt durch ein geheimes, persönliches Kennwort zu ersetzen.

Der zuständige Abteilungsleiter ist verpflichtet, den Administratoren mitzuteilen, wenn der Anwender nicht weiter berechtigt ist, auf die Anlage zuzugreifen. Die Administratoren sperren dann den Zugang zu dem in der Meldung angegebenen Zeitpunkt. Ist der Anwender lediglich zum Zugriff auf bestimmte Teile der Anlage nicht weiter berechtigt, so wird lediglich der betroffene Teil der Anlage gesperrt.

Für die Einrichtung von Zugangsberechtigungen mit Systemverwaltungsbefugnis gemäß Ziff. 11.3 ist die Zustimmung des Generalvikars erforderlich

Die Administratoren berichten dem zuständigen Dezernenten mindestens einmal jährlich oder auf Anforderung über die einer Abteilung oder einem Dezernat zugeordneten Zugangsberechtigungen. Die Abteilungsleiter und Dezernenten prüfen die Zugangsberechtigungen und bestätigen dies den Administratoren.

4. Zugriffsberechtigung

Der Anwender muss, um eine Zugriffsberechtigung zu erhalten, einen Antrag stellen.

Der zuständige Abteilungsleiter muss dem Antrag zugestimmt haben, wenn der Anwender lediglich Zugriff auf Verzeichnisse und Dateien seiner Abteilung benötigt.

Der Dezernent muss dem Antrag zugestimmt haben, wenn der Anwender Zugriff auf Verzeichnisse und Dateien mehrerer Abteilungen innerhalb seines Dezernats benötigt.

Alle betroffenen Dezernenten müssen zugestimmt haben, wenn der Anwender Verzeichnisse und Dateien von Abteilungen mehrerer Dezernate benötigt.

Für die Einrichtung von Zugriffsberechtigungen für Zugangsberechtigte, die nicht Mitarbeiter (Externe z.B. Krankenkassenprüfer, Finanzprüfer) sind, ist die Zustimmung des Dezernenten, der für gewünschte Verzeichnisse und Dateien verantwortlich ist, erforderlich.

Benötigt ein Anwender Zugriff auf einen geänderten Satz von Verzeichnissen und Dateien (z.B. aufgrund Abteilungswechsel, neue Aufgabenbereiche), ist ein Änderungsantrag einzureichen.

Um sicherzustellen, dass die neue Zuweisung von Verzeichnissen und Dateien korrekt ist, hat der Anwender analog zum oben beschriebenen Verfahren die Zustimmung aller betroffenen Abteilungsleiter bzw. Dezernenten einzuholen.

Die Administratoren ändern die Zugriffsberechtigung in der Weise, dass der Anwender lediglich Zugriff auf die im Änderungsantrag bezeichneten Verzeichnisse und Dateien erhält. Alle weiteren Berechtigungen werden entzogen.

Die Abteilungsleiter haben dafür Sorge zu tragen, dass die Administratoren zur Änderung des Zugriffs auf Dateien und Verzeichnisse angewiesen werden, sobald sich die Berechtigung des Anwenders zum Zugriff auf diese Dateien und Verzeichnisse ändert.

Alle Unterlagen, die die Einrichtung, Änderung oder Löschung von Zugriffsberechtigungen betreffen, sind mit Hilfe von Antragsformularen schriftlich bei den Administratoren einzureichen. Sie bewahren diese Anträge sowie die daraufhin ergangenen Entscheidungen auf und dokumentieren die durchgeführten Änderungen (Musterantragsformulare in Anlage).

5. Nutzung der Anlage

Das Bistum Mainz stellt die EDV-Anlagen zur dienstlichen Nutzung bereit.

In der Regel ist eine private Nutzung des EDV-Netzwerks nicht zulässig. Ausnahmen sind in Absprache mit dem Dienstvorgesetzten zu regeln. Dienstliche Belange dürfen nicht berührt und die Daten nicht im System abgespeichert werden (schreibmaschinenähnliche Nutzung).

6. Sicherheitsregeln zur Vermeidung von unbefugten Zugriffen

6.1 Allgemeines

Mit Hilfe der EDV-Anlagen werden Informationen verarbeitet, die hohe Anforderungen an den Datenschutz stellen. Aus diesem Grund ist jeder Benutzer der Anlage verpflichtet, die Sicherheitsrichtlinien strikt einzuhalten. Dies soll den unbefugten Zugriff auf die Anlage und auf die in der Anlage gespeicherten Informationen verhindern.

Alle Anwender und deren zuständige Abteilungsleiter bzw. Dezernenten sind darüber hinaus verpflichtet, ihnen bekannte Sicherheitsprobleme, die zu einem nicht autorisierten Zugang zu den in der Anlage gespeicherten Informationen führen können, unverzüglich an den Generalvikar und die Administratoren weiterzugeben.

6.2 Spezielle Regeln

1. Das mit der Zugangsberechtigung von den Administratoren erhaltene Kennwort zum Zugang zur Anlage ist vom Anwender unverzüglich zu ändern. Das persönliche Kennwort ist geheim zu halten. Es darf unter keinen Umständen an andere Personen, Externe, Kollegen, Vorgesetzte oder Mitarbeiter der EDV-Abteilung weitergegeben werden.

Das geheime Kennwort muss vom Anwender in regelmäßigen Abständen geändert werden. Diese Änderung muss mindestens alle 6 Monate (180 Tage) durchgeführt werden. Für das zu wählende Kennwort gelten folgende Regeln:

- es muss mindestens 6 Zeichen enthalten, von denen zwei Zeichen keine Buchstaben sind
- nach drei aufeinander folgenden, fehlerhaften Eingaben wird die Zugangsberechtigung automatisch gesperrt
- ein bestimmtes Kennwort darf erst nach fünf Kennwortänderungen wieder verwendet werden
- das Kennwort darf nicht niedergeschrieben werden.

Wurde die Zugangsberechtigung gesperrt, kann die Aufhebung der Kennwortsperre bei den Administratoren beantragt werden. Der Antrag kann telefonisch gestellt werden.

Der Administrator darf die Kennwortsperre nur aufheben, wenn ihm der Anrufer persönlich bekannt ist. Ist der Antragsteller persönlich nicht bekannt, kann der Antrag auch durch einen dem Administrator bekannten Mitarbeiter gestellt werden, der sich für den nicht bekannten Mitarbeiter verbürgt.

Wurde das Kennwort vergessen, muss die Zugangsberechtigung des betroffenen Anwenders rückgestellt werden. Hierzu wird durch die Administratoren wieder ein Kennwort voreingestellt, das durch den Anwender sofort zu ändern ist. Es gilt das gleiche Verfahren wie bei der erstmaligen Vergabe einer Zugangsberechtigung. Im Übrigen folgt das Verfahren dem Verfahren bei der Aufhebung der Sperre der Zugangsberechtigung.

Ist ein dem Administrator bekannter Mitarbeiter, der sich für den unbekannten Mitarbeiter verbürgt, nicht vorhanden, so kann die Vergabe eines neuen Kennworts nur auf schriftlichen Antrag erfolgen. Zur Feststellung der Identität ist der Personalausweis vorzulegen.

2. Der Anwender hat dafür Sorge zu tragen, dass ein Zugriff auf die Informationen der Anlage mit Hilfe seiner Kennung in seiner Abwesenheit (z.B. Pausen) nicht möglich ist. Hierzu hat er sich abzumelden oder die Arbeitsstation zu sperren.

3. Es ist untersagt, die Arbeitsplatzsysteme ohne Anwesenheit der Administratoren zu öffnen. An den Arbeitsplatzsystemen dürfen keine Einrichtungen zur elektronischen Kommunikation (z.B. Modems, ISDN-Karten etc.) angeschlossen werden. Arbeitsplatzsysteme dürfen nur durch die Administratoren an das Netzwerk angeschlossen werden.

4. Die Benutzung von Programmen, die zum Ausspähen des Datenverkehrs oder zum Ausspähen oder Erlangen von Kennwörtern geeignet sind, ist verboten.

5. Die Administratoren haben geeignete Zugriffsschutzmaßnahmen einzurichten, die sicherstellen, dass ein nicht-autorisierter Zugriff auf Informationen unter normalen Umständen nicht möglich ist

7. Nutzung von Dateiablagen

7.1 Allgemeines

Dateiablagen sind Verzeichnisse und Laufwerke, die den Anwendern des Netzwerks zur gemeinsamen oder persönlichen Nutzung zur Verfügung stehen. Diese Dateiablagen befinden sich auf zentralen Geräten innerhalb der EDV-Abteilung.

Arbeitsergebnisse oder relevante Zwischenergebnisse sind nach Maßgabe der folgenden Ziffern 7.2 bis 7.4 innerhalb der zentralen Dateiablagen (i.d.R. auf Laufwerk M) zu speichern. Die Speicherung dieser Informationen auf den lokalen Laufwerken der Arbeitsplatzsysteme (z.B. Laufwerk C) ist nicht gestattet, weil die Daten, die lokal abgelegt sind, nicht zentral gesichert sind. Bei einem Austausch des Arbeitsplatzsystems oder einer Störung gehen diese Daten verloren. Die Speicherung auf Wechselmedien (z.B. Disketten, CD-ROMs) der Arbeitsplatzsysteme darf lediglich zu Zwecken des Datenaustausches mit Systemen außerhalb der Vernetzung erfolgen. Das Dienstgeheimnis ist zu wahren.

Die Anwender werden darauf hingewiesen, dass die EDV-Abteilung lediglich eine Datensicherung und somit keine „Archivierung“ durchführt. Archivierung meint die dauerhafte Aufbewahrung von Akten, Vorgängen, Unterlagen etc. Insofern sind diese wie bisher in Papierform auszudrucken.

7.2 Gemeinsame Dateiablage

Es werden gemeinsame Dateiablagen zur Nutzung durch die Organisationseinheiten (Abteilungen, Dezernate, Arbeitsgruppen etc.) eingerichtet. Diese strukturieren die Ablagebereiche eigenständig und eigenverantwortlich. Sie werden dabei von den Administratoren unterstützt.

Die Administratoren sind zuständig, die technische Umsetzung für die von den Organisationseinheiten gewünschten Änderungen am jeweiligen Ablage- und Zugriffsplan durchzuführen. Hierzu werden die Administratoren mit den notwendigen Zugriffsrechten ausgestattet. Sie sind berechtigt, auf die dort gespeicherten Informationen im erforderlichen Umfang Zugriff zu nehmen. Sie bedürfen hierbei der Zustimmung des zuständigen Dezernenten.

Zur Verwaltung der Dateiablagen des Bischofshauses und des Offizialats werden getrennte Zugangsberechtigungen geschaffen, die den Administratoren nicht bekannt sind. Die Verwaltung dieser Dateiablagen unterliegt vollständig dem Bischofshaus und dem Offizialat. Den Administratoren ist kein Zugriff auf die Inhalte dieser Ablagen gestattet, sofern keine anderslautende Anweisung des Bischofshauses oder des Offizialats vorliegt. Liegt eine solche Anweisung vor, so werden die Änderungen im Beisein eines Mitarbeiters des Bischofshauses bzw. des Offizialats mit Hilfe der separaten Zugangsbe-

rechtigungen durchgeführt. Es ist nicht gestattet, den Administratoren die getrennten Zugangsberechtigungen zu überlassen.

7.3 Persönliche Dateiablage

Jedem Anwender des Netzwerks steht eine persönliche Dateiablage (Laufwerk U) zur Verfügung, auf die weder die Administratoren noch andere Anwender Zugriff erhalten. Ziffer 7.4 ist zu beachten.

Auf Weisung des vorgesetzten Dezernenten kann in dringenden Fällen der Zugriffsschutz auf diese Bereiche in der Weise aufgehoben werden, dass ein vom Dezernenten benannter Anwender auf die Daten Zugriff erhält (z.B. im Fall längerer Krankheit).

7.4 Schutzbereiche

Mitarbeiter, die den Schutzbereichen zugeordnet sind, verarbeiten Informationen höchster Vertraulichkeit. Für diese Gruppe von Anwendern gelten Sonderregelungen, die mit den jeweiligen Bereichen und den Administratoren umgesetzt werden.

8. Elektronische Kommunikation / E-Mail- / Internetnutzung

8.1 Allgemeine Hinweise

Die EDV-Anlage des Bistums verfügt über eine Reihe von Einrichtungen, die die elektronische Kommunikation (z.B. E-Mail, Video-, Audio-Übertragungen) ermöglichen und deren Nutzung den Anwendern möglich ist. Die Nutzung dieser Einrichtungen unterliegt verschiedenen gesetzlichen Bestimmungen, die durch die Nutzer der Anlage eingehalten werden müssen (KDO, Telekommunikationsgesetze).

Zum Schutz der EDV-Anlage vor unbefugtem Eindringen und zum Schutz vor schädlichen Inhalten werden automatisierte Kontrollen des Datenverkehrs durchgeführt.

8.2 Teilnahme auswärtiger Stellen am internen Kommunikationssystem

Die EDV-Anlage erlaubt die Anbindung von Außenstellen des Bischöflichen Ordinariates an das interne Kommunikationssystem der EDV-Anlage.

Voraussetzung der Anbindung dieser Außenstellen ist die Abgabe einer Verpflichtungserklärung der Mitarbeiter, diese Ordnung sorgfältig einzuhalten, soweit sich diese auf die Punkte 1 – 5 und 6 (Ausnahme 6.2.3.) bezieht. Die Verpflichtungserklärung bezieht die EDV-Dienstvereinbarung vom 23.04.2001 ein.

Die Anbindung ist beim Lenkungsausschuss zu beantragen. Die Durchführung der Anbindung bedarf der Zustimmung der Dezernentenkonferenz. Die Berechtigung kann durch Beschluss der Dezernentenkonferenz ohne Angabe von Gründen aufgehoben werden.

8.3 Bedeutung der E-Mail-Funktion

Rechtsverbindliche Äußerungen durch E-Mails können nur im Bereich

- der Kernvernetzung
- der am internen Kommunikationssystem angeschlossenen Außenstellen
- und vergleichbarer anderer sicherer Kommunikationssysteme

verwendet werden. Sie sind mit der digitalen Signatur des Ausstellers zu versehen und als rechtsverbindliche Äußerung zu kennzeichnen. Durch übergreifendes Recht kann anderes geregelt werden.

Für die Kommunikation mit allen anderen Stellen werden E-Mails als ein Medium der flüchtigen und spontanen Kommunikation angesehen, das insoweit mit dem Telefon vergleichbar ist. Bei rechtsverbindlichen Äußerungen ist die Verwendung von E-Mails nur bis zu einer Wertobergrenze von 100,– € ausreichend. Bei Beträgen, die darüber hinausgehen, sind rechtsverbindliche Erklärungen stets in herkömmlicher Papierform abzugeben, sofern mit der jeweiligen Stelle keine andere Vereinbarung getroffen wurde.

Vertrauliche interne Informationen, insbesondere personenbezogene Daten dürfen nur im Bereich der Kernvernetzung, der am internen Kommunikationssystem angeschlossenen Außenstellen und vergleichbarer anderer sicherer Kommunikationssysteme per E-Mail versandt werden.

An alle anderen Stellen dürfen keine vertraulichen internen Informationen, insbesondere personenbezogene Daten versandt werden.

8.4 Internet-Nutzung

Die Internetnutzung regeln die jeweiligen Dienstvereinbarungen über die Einführung und den Einsatz von EDV- Hard- und Software in den angeschlossenen Einrichtungen.

Das Versenden von vertraulichen internen Informationen, insbesondere personenbezogene Daten ist nicht gestattet.

9. Einsatz von Software

9.1 Allgemeines

Um die Kooperationsmöglichkeiten der Nutzer zu optimieren und die Kosten für den Betrieb der Anlagen zu minimieren, ist es notwendig, die Entscheidung über den Einsatz bestimmter Software zu koordinieren. Diese Aufgabe wird durch den Lenkungsausschuss wahrgenommen.

9.2 Kategorisierung und Meldung von Software

Jede Software fällt in eine der drei folgenden Kategorien:

Kategorie C

- Software, die zu Testzwecken eingesetzt wird fällt automatisch in diese Kategorie.
- Die Testphase ist begrenzt auf maximal drei Monate.
- Danach erlischt das Verwendungsrecht.

Kategorie B

- Wenn Software nach der Testphase an einem oder mehreren Arbeitsplätzen eingesetzt werden soll, und sie zur Erlangung von Arbeitsergebnissen unverzichtbar ist, muss sie wie in 9.4 beschrieben beantragt werden.

Kategorie A

- Gleiches gilt für Software, die an jedem Arbeitsplatz der EDV-Anlage zur Verfügung stehen soll.

Die Administratoren sind zuständig für Betrieb und Pflege der Software der Kategorie A und B.

Weiter ist zu jeder eingesetzten Software ein Verantwortlicher (Software-Verantwortlicher) zu nennen, der den Anwendern der Software bei Anwendungsfragen zur Verfügung steht.

9.3 Anzeigepflicht

Der Einsatz von Software auf einem Arbeitsplatzsystem (Kategorie C) ist den Administratoren zu melden (Anzeigepflicht). Unter diese Anzeigepflicht fallen auch Downloads aus dem Internet. Zuständig für die Meldung, ist derjenige Anwender, der die Software installiert.

Die Anzeige entbindet nicht von der Verpflichtung des Anwenders, nur lizenzierte Software zu verwenden und auf Anforderung einen Nachweis der Lizenz zu liefern.

9.4 Durchführung der Kategorisierung

Entsteht an den Arbeitsplätzen eines Dezernats der Bedarf, ein Problem mit Hilfe einer noch nicht vorhandenen Software zu lösen, so entscheidet zunächst der Dezernent, ob das Problem mit Hilfe der EDV gelöst werden soll.

Bei Zustimmung des Dezernenten ist der Lenkungsausschuss über das Problem und die mögliche Lösung des Problems (z.B. käufliche Software, Entwicklungsauftrag) zu informieren und ein verantwortlicher Betreuer im Sinne der Ziffer 9.2. vorzuschlagen.

Der Lenkungsausschuss prüft das Problem und den Lösungsweg unter den Aspekten:

- Kann das Problem mit bereits vorhandenen Mitteln gelöst werden?
- Besteht von Seiten anderer Organisationseinheiten ein identischer/ähnlicher Bedarf?
- Durchführung einer Kosten-/Nutzenanalyse

- Technische Prüfung des Lösungswegs in Zusammenarbeit mit der EDV-Abteilung
- Ggf. Empfehlung eines alternativen Lösungswegs

Der Lenkungsausschuss kann mit Zustimmung des Generalvikars die Prüfung des Lösungsansatzes auf diese Aspekte an Dritte delegieren und Entscheidungen auf Basis der Empfehlungen Dritter treffen.

Kann das Problem mit bereits vorhandener Software gelöst werden, so wird der Einsatz der beantragten Software abgelehnt, da davon auszugehen ist, dass die Nutzung unterschiedlicher Systeme zur Lösung identischer oder ähnlicher Probleme mit Nachteilen (Kooperationsmöglichkeiten, Kosten) verbunden ist. Der Lenkungsausschuss kann auch aus anderen Gründen einen Antrag auf Kategorisierung ablehnen. Die Ablehnung wird dem Antragsteller mitgeteilt.

Das Votum des Lenkungsausschusses wird, nach Zustimmung der zuständigen MAV, der Dezernentenkonferenz mitgeteilt.

Die Dezernentenkonferenz entscheidet über das weitere Vorgehen.

Auf der Grundlage der Entscheidungen der Dezernentenkonferenz beauftragt der Vorsitzende des Lenkungsausschusses die für die technische Umsetzung verantwortlichen Stellen (z.B. Administratoren, Softwareverantwortliche) mit der Umsetzung. Die beauftragten Stellen sind verpflichtet, dem Lenkungsausschuss nach dessen Maßgabe über die Umsetzung zu berichten.

10. Lenkungsausschuss

10.1 Aufgaben

Aufgabe des Lenkungsausschusses ist die Koordinierung und Fortentwicklung der EDV-Nutzung im Geltungsbereich der EDV-Ordnung.

Der Lenkungsausschuss protokolliert seine Sitzungen.

10.2 Besetzung und Vorsitz

Das Bischofshaus, das Offizialat und Dezernate mit weniger als zehn Mitarbeitern zum Ersten sowie die Dotation und die Domkirche St. Martin zum Zweiten und die Mitarbeitervertretungen zum Dritten entsenden je einen gemeinsamen Vertreter.

Alle übrigen Dezernate des Ordinariates benennen jeweils einen Vertreter für den Lenkungsausschuss. Der Leiter der EDV-Abteilung ist kraft Amtes Mitglied des Lenkungsausschusses.

Der Vorsitzende des Lenkungsausschusses wird von der Dezernentenkonferenz ernannt.

Der Vorsitzende des Lenkungsausschusses kann Fachberater, insbesondere Systemberater, Internetbeauftragte, Administratoren hinzuziehen.

11. EDV-Abteilung

11.1 Allgemeines

Die EDV-Abteilung ist für den technischen Betrieb der EDV-Anlage zuständig. Dies umfasst alle Aspekte, die für die Entwicklung, Aufrechterhaltung und Absicherung des Betriebs notwendig sind. Darüber hinaus unterstützen die Mitarbeiter der EDV-Abteilung die Anwender durch Schulungen und Beratung.

11.2 EDV-Fachbetreuer

Zur Entlastung der EDV-Abteilung bei der Benutzerunterstützung wird in jeder Organisationseinheit mindestens ein Fachbetreuer für die Nutzung der EDV-Anlagen vom jeweiligen Dezernenten benannt.

Aufgabe des Fachbetreuers ist es, die Nutzer der EDV-Anlage bei auftretenden Problemen und Anforderungen zuerst zu unterstützen.

11.3 Administratoren

Die Administratoren genießen eine besondere Vertrauensstellung, die auf ihrer technischen Möglichkeit beruht, Sicherheits- und Zugriffsschutzverfahren innerhalb der EDV-Anlage zu modifizieren.

Sie sind verpflichtet sicherzustellen, dass die von ihnen durchgeführten Maßnahmen, dem Sinn der Sicherheits- und Zugriffsschutzmaßnahmen nicht entgegenstehen. Sie sind berechtigt, für die Durchführung von Tätigkeiten, die die Sicherheits- und Zugriffsschutzmaßnahmen betreffen, schriftliche Anweisungen zu verlangen und diese im Zweifelsfall durch den Generalvikar bestätigen zu lassen.

Die Inspektionen des Sicherheitsausschusses bestätigen der EDV-Abteilung die korrekte Durchführung der Sicherheitsmaßnahmen.

11.4 Systempflege und Entstörungsmaßnahmen

Die EDV-Abteilung ist berechtigt, zur Durchführung von Tätigkeiten zur Pflege und zum Ausbau der EDV-Anlage, Teile der EDV-Anlage oder das Gesamtsystem zeitweise außer Betrieb zu nehmen.

Diese Maßnahmen unterliegen verschiedenen Prioritäten, die von den Mitarbeitern der EDV-Abteilung nach Maßgabe der Umstände einzuhalten sind:

Priorität 1:

Entstörung der Sicherheitseinrichtungen der EDV-Anlage

Werden Fehler in den Sicherheitseinrichtungen festgestellt, die die Sicherheit der EDV-Anlage gefährden, ist die EDV-Abteilung verpflichtet, die Entstörung unverzüglich

vorzunehmen. Bis zur erfolgten Entstörung, werden alle Einrichtungen, die von der Störung der Sicherheitseinrichtungen betroffen sind (insbesondere Einrichtungen zur Kommunikation außerhalb des Netzwerks) unverzüglich deaktiviert.

Priorität 2:

Entstörung zentraler Einrichtungen der EDV-Anlage (Zentrale technische Einrichtungen und Software der Kategorie A)

Werden Fehler in diesem Bereich festgestellt, die die Funktionsfähigkeit der EDV-Anlage ganz oder teilweise beeinträchtigen, werden die Entstörungsmaßnahmen sofort eingeleitet. Sind zur Entstörung zeitweise weitere Funktionsbeeinträchtigungen zu erwarten, kann die Entstörung nach Ermessen der EDV-Abteilung zu einem späteren Zeitpunkt durchgeführt werden.

Priorität 3:

a) Pflege zentraler Einrichtungen der EDV-Anlage
(Zentrale technische Einrichtungen und Software der Kategorie A)

Um die Funktionsfähigkeit der zentralen Einrichtungen der EDV-Anlage aufrecht zu erhalten, sind Maßnahmen zur (routinemäßigen oder außerordentlichen) Pflege von zentralen Einrichtungen mit hoher Priorität durchzuführen. Sofern die Maßnahmen mit Funktionseinbußen verbunden sind, sind sie den Anwendern mit einer Ankündigungsfrist von zwei Arbeitstagen mitzuteilen.

b) Pflege und Entstörung weiterer Einrichtungen der EDV-Anlage
(Besondere technische Einrichtungen und Software der Kategorie B)

Dies sind erforderliche Pflege- oder Entstörungsmaßnahmen im Bereich technischer Einrichtungen und im Bereich von Software, die der Kategorie B zugeordnet ist. Sofern die Maßnahmen mit Funktionseinbußen verbunden sind, sind sie den Anwendern mit einer Ankündigungsfrist von zwei Arbeitstagen mitzuteilen.

Priorität 4:

Entstörung von Arbeitsplatzsystemen
(Einzelne Arbeitsplatzsysteme)

Treten technische Probleme an den Arbeitsplatzsystemen auf, sind diese spätestens nach Abschluss von Arbeiten der Prioritäten 1 – 3 zu lösen.

Folgende Maßnahmen stehen zur Verfügung:

- Versuch der Fehlerbehebung am Arbeitsplatz durch Modifikation des Systems. Maximale Zeitdauer des Entstörungsversuches: 1 Arbeitsstunde
- Neuinstallation des Systems nach vorheriger vollständiger Löschung oder alternativ
- Austausch des Systems

Sofern spezifische Software auf dem System eingesetzt wird, unterstützen die Software-Verantwortlichen, Fachbetreuer und Administratoren den Anwender bei der Neueinrichtung dieser Software.

Treten Störungen auf, die den Prioritäten 1 und 2 zugeordnet sind, kann die EDV-Abteilung nachgeordnete Aufgaben abbrechen.

11.5 Benutzerunterstützung, Beratung und Schulungen

Die EDV-Abteilung, die Software-Verantwortlichen und die Fachbetreuer unterstützen die Anwender durch Beratung, gegebenenfalls Schulungsmaßnahmen und bei technischen Problemen.

12. Sicherheitsausschuss

12.1 Aufgabe

Aufgabe des Sicherheitsausschusses ist die Überwachung der Sicherheitsvorkehrungen der EDV-Anlage im Hinblick auf Datenverlust und unbefugten Zugriff.

12.2 Besetzung

Der Sicherheitsausschuss umfasst fünf Mitglieder, die jeweils vom Bischofshaus, vom Offizialat, vom Ordinariat und von den Mitarbeitervertretungen benannt werden und nicht der EDV-Abteilung angehören dürfen. Als fünftes Mitglied ernennt die Bistumsleitung ein externes, kompetentes Mitglied.

12.3 Inspektion

Der Sicherheitsausschuss inspiziert mindestens einmal jährlich.

Die Inspektionen umfassen:

- die Kontrolle der Benutzerverwaltung und deren Dokumentation
- die Kontrolle der Sicherheitseinrichtungen des Netzwerks (z.B. Firewall, Virenschutz) auf korrekten Betrieb und Vollständigkeit der Dokumentation
- die Kontrolle der Zugriffsrechte auf Ressourcen der EDV-Anlage
- die Kontrolle sonstiger sicherheitsrelevanter Anlagen und Programme

Die Inspektion kann nach Maßgabe des Sicherheitsausschusses in Form von Stichproben oder vollständig erfolgen.

Die EDV-Abteilung ist verpflichtet, die Inspektion durch den Sicherheitsausschuss in jeder Form zu unterstützen.

12.4 Mängelbeseitigung

Der Sicherheitsausschuss ist verpflichtet, der EDV-Abteilung vorhandene Mängel schriftlich anzuzeigen. Sofern der Sicherheitsausschuss Mängel feststellt, ist die EDV-Abteilung verpflichtet, die Beseitigung der Mängel umgehend zu veranlassen. Der Abschluss der Mängelbeseitigung ist dem Sicherheitsausschuss anzuzeigen. Dieser führt eine abschließende Kontrolle der bemängelten Sachverhalte durch.

Nach Abschluss der Mängelbeseitigung entlastet der Sicherheitsausschuss die EDV-Abteilung.

12.5 Berichtspflicht

Der Sicherheitsausschuss berichtet der Dezernentenkonferenz über die Ergebnisse der Inspektionen. Die Berichte des Sicherheitsausschusses sind vertraulich und als Dienstgeheimnisse einzustufen.

13. Datenschutzbeauftragte und MAVen

Die Befugnisse des Datenschutzbeauftragten und die gesetzlichen Beteiligungsrechte der MAVen bleiben von dieser Ordnung unberührt.

Diese Ordnung tritt mit Ablauf des Tages ihrer Unterzeichnung in Kraft. Gleichzeitig tritt die „Vorläufige EDV-Ordnung des Bistums Mainz“ außer Kraft.

Mainz, den 21. Mai 2002

Generalvikar

Anlage 1
Eigenständige Organisationseinheiten

- Bischofshaus
- Bischöfliches Domkapitel
- Bischöfliche Dotation
- Dezernate des Ordinariates
- Martinus-Bibliothek
- Offizialat

Anlage 2

Formular zur Zugangsberechtigung

ZUGANGSBERECHTIGUNG Bischöfliches Ordinariat Mainz

☐ Einrichtung ☐ Änderung ☐ Löschung

Name: _____ **Vorname:** _____

Dezernat: _____ **Abteilung:** _____ **Referat:** _____

zus. Dezernat: _____ **Abteilung:** _____ **Referat:** _____

mit Wirkung vom: _____

Die Zugangsberechtigung für das PC-Netzwerk gilt

☐ **unbefristet** ☐ **bis** _____

BESONDERE ZUGANGSBERECHTIGUNGEN

☐ **GROSSRECHNER**

(Anwendungsprogramme angeben) _____

☐ **INTERNET (WWW. Anbindung)**
E-Mail Funktion ist für jeden verfügbar

(Begründung) _____

Die Datenschutzbestimmungen der KDO,die EDV-Ordnung und die Dienstvereinbarung über die Einführung und Einsatz von EDV Hard- und Software im Bischöflichen Ordinariat Mainz vom 23.04.2001 habe ich zur Kenntnis genommen.

Datum: _____ Unterschrift des Mitarbeiters: _____

Abteilungsleiter: _____ DezernentIn: _____

(Falls Zugänge auch in anderen Dezernaten erforderlich) DezernentIn: _____

Verteiler:

Mitarbeiter
EDV-Abteilung
(Nichtzutreffendes streichen)

Abteilungsleiter / Dezernent
M A V

(Nur von der EDV-Abteilung auszufüllen:)

Dem Benutzer wird folgende Benutzerkennung für die Anmeldung in Windows-NT zugewiesen: _____

Formular zur Zugriffsberechtigung

ZUGRIFFSBERECHTIGUNG Bischöfliches Ordinariat Mainz

☐ Einrichtung ☐ Änderung ☐ Löschung

Name: _____ **Vorname:** _____

Dezernat: _____ **Abteilung:** _____ **Referat:** _____

zus. Dezernat: _____ **Abteilung:** _____ **Referat:** _____

mit Wirkung vom: _____

Die Zugriffsberechtigung gilt

☐ **unbefristet** ☐ **bis** _____

ZUGRIFFSBERECHTIGUNGEN

(bitte genauen Pfad z.B.:M:\allgemein\test angeben)

		Vollzugriff	Schreibzugriff	Lesezugriff
☐ **VERZEICHNIS**	_____	☐	☐	☐
☐ **VERZEICHNIS**	_____	☐	☐	☐
☐ **VERZEICHNIS**	_____	☐	☐	☐
☐ **VERZEICHNIS**	_____	☐	☐	☐

Zustimmung zur Erteilung der Zugriffsberechtigung

Abteilungsleiter: _____ DezernentIn: _____
(=Vorgesetzter) (wenn abteilungsübergreifender Zugriff)

(Falls Zugriffe auch in anderen Dezernaten erforderlich) DezernentIn: _____

Verteiler:

Mitarbeiter Abteilungsleiter / Dezernent

EDV-Abteilung M A V

(Nichtzutreffendes streichen)

(Nur von der EDV-Abteilung auszufüllen:)

Dem Benutzer wurde Zugriff erteilt _____ _____
Datum Unterschrift