Rundschreiben des Landeskirchenamtes an die Kirchengemeinden und Kirchenkreise betreffend

- **Empfehlungen zum Datenschutz und zur Datensicherheit für die Benutzung von PC**
- **Merkblatt zur datenschutzgerechten Gestaltung von Passwörtern**
- **Merkblatt zum Datenschutz und zur Datensicherheit betreffend Computerviren**

Vom 22. März 1999 (Az.: A 14-03/01.09)

[1]In den letzten Jahren hat die Entwicklung der Informationstechnologie die Arbeitswelt stark verändert. [2]Personenbezogene Daten werden inzwischen in der kirchlichen Verwaltung überwiegend automatisiert verarbeitet, d. h. sie werden hierzu in Dateien gespeichert und mittels Arbeitsplatzcomputer (PC) verarbeitet. [3]Die Informationstechnologie stellt heute eine Grundvoraussetzung für ein effektives Handeln der kirchlichen Stellen dar. [4]Zugleich muss aber dem Schutz der verarbeiteten Daten erhöhte Aufmerksamkeit zukommen.

[1]Ein angemessener Schutz der durch die Informationstechnik vorgehaltenen Daten kann nur durch eine enge Zusammenarbeit aller handelnden Personen der kirchlichen Stelle sichergestellt werden. [2]Die kirchliche Stelle hat nach § 9 des Kirchengesetzes über den Datenschutz der EKD[1] die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den datenschutzrechtlichen Anforderungen zu entsprechen. [3]In diesem Zusammenhang ist es auch notwendig, regelmäßig alle am PC arbeitenden Personen über die datenschutzrechtlichen Gefahren aufzuklären. [4]Dadurch steigt auch das Verantwortungsbewusstsein der Mitarbeiterinnen und Mitarbeiter und es kann dem Zweck des Datenschutzes, den Einzelnen vor Benachteiligungen in den Persönlichkeitsrechten zu schützen, besser entsprochen werden.

[1]Die beigefügten Empfehlungen zum Datenschutz und zur Datensicherheit für die Benutzung von PC wenden sich an die PC-Benutzerinnen und PC-Benutzer und geben ihnen Tipps für den sicheren Umgang mit dem PC. [2]Sie sollen die Benutzerinnen und Benutzer für die Belange der PC-Sicherheit sensibilisieren und allgemeine Schutzmöglichkeiten für den PC-Einsatz aufzeigen, unabhängig davon ob es sich um einen Einzelplatz-PC oder um einen vernetzten PC handelt.

[1]Häufig werden zu einfache Passwörter als Zugangsschutz zum PC benutzt. [2]Auch sind viele Benutzerinnen und Benutzer von PC oft nicht ausreichend darüber unterrichtet, wie man einen Virenbefall erkennt, sich gegebenenfalls verhält und wie man vorbeugend tätig

1 Nr. **850**

sein kann. [3]Daher haben wir in besonderen Merkblättern die Themen „Passwortgestaltung/ Virenschutz“ aufgegriffen.

Wir schlagen vor, die Empfehlungen und die Merkblätter allen Mitarbeiterinnen und Mitarbeitern zuzuleiten, die an PC-Arbeitsplätzen arbeiten.

Empfehlungen der Evangelischen Kirche von Westfalen zum Datenschutz und zur Datensicherheit für die Benutzung von Arbeitsplatzcomputern (PC)

– Stand 01.03.1999 –

[1]Diese Hinweise zum Thema Datensicherheit und Datenschutz sind für die Benutzerinnen und Benutzer von PC zusammengestellt worden. [2]Ihre Nichtbeachtung kann arbeits-, dienst- oder strafrechtliche Maßnahmen zur Folge haben. [3]Auch muss mit Schadensersatzansprüchen gerechnet werden, die aufgrund von Verletzungen von Datenschutzbestimmungen bzw. von Persönlichkeitsrechten geltend gemacht werden können.

Jede Mitarbeiterin und jeder Mitarbeiter trägt für vorschriftsgemäße Ausübung der jeweiligen Tätigkeit die volle datenschutzrechtliche Verantwortung.

[1]Alle Mitarbeiterinnen und Mitarbeiter dürfen Daten oder Aufzeichnungen nur zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeiten oder nutzen. [2]Eine Offenbarung personenbezogener Daten gegenüber anderen kirchlichen Stellen, sonstigen Stellen oder Personen ist nur zulässig, wenn es hierfür eine Rechtsgrundlage gibt.

[1]Der Umgang mit Daten und Informationen erfordert von jeder Mitarbeiterin und jedem Mitarbeiter ein hohes Maß an Verantwortungsbewusstsein; die sorgsame und vertrauliche Behandlung von Daten ist der wichtigste Grundsatz der Informationsverarbeitung. [2]Insbesondere die Sammlung, Aufbereitung und Verwendung personenbezogener Daten unterliegen einer erhöhten Schutzbedürftigkeit.

Für die Bedienung des PC ist die Benutzerin oder der Benutzer verantwortlich.

Soweit mehrere Mitarbeiterinnen und Mitarbeiter auf einen PC zugreifen, ist die Mitarbeiterin oder der Mitarbeiter zu benennen, der verantwortlich ist für

* Beginn und Ende der Arbeiten am System,
* Passwortschutz,
* Datensicherung und Aufbewahrung der Datenträger, soweit ein Diskettenlaufwerk vorhanden ist.

Die Benutzerinnen und Benutzer sind für die Einhaltung der bereichsspezifischen und allgemeinen Datenschutzbestimmungen in ihrem Bereich verantwortlich.

Die allgemeinen Datenschutzbestimmungen ergeben sich insbesondere aus dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)[1] sowie

den ergänzenden Durchführungsbestimmungen der EKvW (DSVO)[1] Weitere bereichsspezifische Datenschutzvorschriften sind in den jeweiligen Fachgesetzen und Durchführungsverordnungen enthalten.

[1]Nach § 9 DSG-EKD haben kirchliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Kirchengesetzes, insbesondere die in der Anlage zu diesem Kirchengesetz genannten Anforderungen, zu gewährleisten. [2]In der Anlage zu § 9 sind die 10 Gebote zum Umgang mit personenbezogenen Daten enthalten, die für die Benutzerinnen und Benutzer zum besseren Verständnis wiedergegeben werden:

„Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

---

1 Nr. **850**
1 Nr. **852**

10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).“

[1]Für die PC-Benutzerinnen und PC-Benutzer wurden 10 Regeln mit Tipps für den sicheren Umgang mit dem PC aufgestellt. [2]Diese 10 Regeln sollen die Benutzerinnen und Benutzer für die PC-Sicherheit sensibilisieren und allgemeine Schutzmöglichkeiten für den PC-Einsatz (gleichgültig ob Einzelplatz-PC oder vernetzter PC) aufzeigen.

10 Sicherheitsregeln für die Benutzerinnen und Benutzer eines PC[1]

1. Schützen Sie den APC vor der Benutzung durch Unbefugte und verhindern Sie beim Verlassen des Arbeitsplatzes die unberechtigte Benutzung von Programmen und Daten!

Begründung:

[1]Wenn die PC frei zugänglich aufgestellt sind, ist die missbräuchliche Nutzung der PC und der Daten leicht möglich. [2]Der Missbrauch kann mit allen Rechten und Möglichkeiten der PC-Benutzer erfolgen. [3]Bei Netzanschluss und Diskettenstation der PC bestehen zusätzliche Gefahren für das Netz und die PC, da z. B. Programm- und Datendisketten mit Viren über den einzelnen PC in das Netz eingebracht werden können.

Mögliche Maßnahmen:	Erläuterung:
Bei Arbeitsbeginn: ☝ Achten Sie auf mögliche Änderungen und Beschädigungen am Gerät sowie seinen Anschlüssen und Verbindungen!	Durch eine einfache Sichtkontrolle können Manipulationen oder Beschädigungen an Geräten und Leitungen erkannt werden.
☝ Verwenden Sie ein Passwort!	Durch die Verwendung eines Passwortes wird der Zugriff Unbefugter auf Anwendungen und Informationen erschwert.
☝ Stellen Sie ggf. fest, wann Ihr PC das letzte Mal benutzt wurde (dies setzt oft den entsprechenden Einsatz eines PC-Sicherheitsproduktes voraus)!	Wird auf dem Bildschirm der Zeitpunkt der letzten PC-Nutzung angezeigt, können Sie erkennen, ob und ggf. wann andere Personen als Sie den PC benutzt haben.

1 Die 10 Sicherheitsregeln beruhen auf Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit dem Dienstsitz in Bonn, die für die tägliche Arbeit im kirchlichen Bereich entsprechend angepasst werden.

Mögliche Maßnahmen:	Erläuterung:
Bei Arbeitsunterbrechung: ☝ Nutzen Sie Bildschirmschoner mit Passwortschutz (z. B. die von PC-Sicherheitsprodukten oder des unter Windows vorhandenen)!	[1]Ein Bildschirmschoner verhindert den Einblick Unbefugter in Ihre Arbeit. [2]Er wird bei Nichtbenutzung von Tastatur oder Maus nach einer vorgestellten Zeit aktiviert. [3]Der Passwortschutz sorgt dafür, dass nur derjenige, der das Passwort kennt, den Bildschirmschoner abschalten kann.
☝ Nutzen Sie die „Hot-Key“-Funktion!	Eine definierbare Tastenkombination bzw. Mausposition, die auch „Hot-Key“ genannt wird, ermöglicht es, den Bildschirmschoner sofort zu aktivieren.
☝ Machen Sie Gebrauch vom Tastaturschloss am PC und nehmen Sie den Schlüssel mit!	Das Tastaturschloss verhindert die Umgehung des Passwortschutzes eines Bildschirmschoners und bietet somit zusätzlichen Schutz.
☝ Wenn Sie Ihr Büro verlassen, schließen Sie es ab!	Das Verschließen der Bürotür bewirkt bei kurzfristiger Abwesenheit vom Arbeitsplatz einen zusätzlichen Schutz.
Beim Verlassen des Arbeitsplatzes: ☝ Schließen Sie alle Anwendungen und trennen Sie ggf. bestehende Netzverbindungen, häufig mit dem Befehl „logout“!	Nur wenn alle Anwendungen geschlossen sind und ein „logout“ durchgeführt wurde, können alle Schutzmechanismen den unbefugten Zugriff zum PC verhindern.
☝ Schalten Sie den PC aus!	Beim Einschalten des PC wird eine evtl. installierte Sicherheitsfunktion, beispielsweise die Abfrage eines Passwortes, aktiviert.

2. Führen Sie regelmäßige Datensicherungen durch, wenn Ihr PC nicht im Netzwerk arbeitet!

Begründung:

Soweit Sie selber für die Datensicherung verantwortlich sind, sollten Sie, wenn Sie mit den Daten arbeiten, täglich eine Datensicherung vornehmen, um für den Fall eines Verlustes (z. B. Crash der Festplatte) oder einer Manipulation von Daten (z. B. von Viren) eine Schadensbegrenzung durch die Verfügbarkeit eines früheren Datenstands vornehmen zu können.

Mögliche Maßnahmen:	Erläuterung:
☝ Erstellen Sie von allen Daten Sicherungskopien (Back-Up)!	Durch Sicherungskopien werden Daten, die sich ansonsten nur auf der Festplatte des PC befinden, zusätzlich auf einem Datenträger vorgehalten.
☝ Sichern Sie alle Verarbeitungsdaten regelmäßig auf Sicherungskopien gemäß den sachlichen Erfordernissen (z. B. nach dem 3-Generationen-Prinzip, wobei immer die 3 letzten Sicherungen vorliegen)!	[1]Bei Verarbeitungsdaten kann durch Aufsetzen auf einen früheren Stand der aktuelle Stand mit vertretbarem Aufwand wiederhergestellt werden. [2]Die Häufigkeit von Sicherungen richtet sich u.a. nach dem Umfang der Änderungen der Originaldaten. [3]Nur durch das Speichern von mindestens zwei Generationen lässt sich sicherstellen, dass für den Fall eines Fehlers während der Sicherung eine weitere Sicherungskopie zur Verfügung steht.
☝ Von Programmen sollte vor der Erstinstallation eine Sicherungskopie erstellt werden!	Sollte die Originalversion des Programms zu einem späteren Zeitpunkt fehlerhaft sein, kann auf die Sicherungskopie zurückgegriffen werden.
☝ Nutzen Sie bei der Herstellung von Sicherungskopien Programme, die gewährleisten, dass die Kopie mit dem Original übereinstimmt („Verify“-Funktion)!	Nur durch eine sofortige Prüfung der gesicherten Informationen bei der Herstellung der Sicherungskopie (z. B.: „Verify“-Funktion) kann gewährleistet werden, dass die Sicherungsbestände auch tatsächlich den Originaldaten entsprechen.
☝ Bewahren Sie die Sicherungsdatenträger räumlich getrennt von den Arbeitskopien, geschützt und verfügbar auf!	[1]Eine Sicherungskopie ist nur dann hilfreich, wenn sie im Bedarfsfall auch verfügbar ist. [2]Die räumlich getrennte Unterbringung, z. B. in einem anderen Brandabschnitt oder in einem anderen Gebäude bewirkt, dass im Brandfall die Sicherungskopien nicht vernichtet werden.

Mögliche Maßnahmen:	Erläuterung:
☝ Überprüfen Sie regelmäßig die Verwendbarkeit der Sicherungskopien!	[1]Informationen auf magnetischen Datenträgern können sich während der Lagerung verändern. [2]Schleichende Veränderungen (z. B. der Spurlage) in Laufwerken können das Lesen alter Kopien erschweren oder verhindern.

3 Gehen Sie verantwortungsvoll mit den vorgesehenen Schutzmöglichkeiten für den PC um!.

Begründung:

Wenn die Schutzmechanismen nicht verantwortungsbewusst genutzt werden, besteht die gleiche Gefährdung des PC, des Netzes, der Programme und Daten wie bei PC-Nutzung ohne Schutzmechanismen.

Mögliche Maßnahmen:	Erläuterung:
☝ Halten Sie Passwörter geheim und lassen Sie sich bei der Eingabe eines Passwortes nicht von Unbefugten auf die Finger schauen.	[1]Ein Passwort kann seine Schutzfunktion nur dann erfüllen, wenn es geheim gehalten wird. [2]Die Verbreitung eines einmal bekannt gegebenen Passwortes ist nicht kontrollierbar. [3]Legen Sie auf keinen Fall Passwörter auf eine Funktionstaste!
☝ Benutzen Sie „gute“ Passwörter!	[1]Passwörter wollen nicht trivial sein, wie z. B.: 123456 oder das eigene Geburtsdatum. [2]Ein gutes Passwort sollte mindestens 6 Zeichen lang sein, Sonderzeichen enthalten und keiner Systematik unterliegen.

Mögliche Maßnahmen:	Erläuterung:
☝ Wechseln Sie das Passwort mindestens vierteljährlich und ändern Sie Ihr Passwort sofort, wenn eine andere Person davon Kenntnis erlangt hat!	[1]Es ist nicht mit letzter Sicherheit auszuschließen, dass Unbefugte trotz aller Vorsicht Kenntnis von Ihrem Passwort erhalten. [2]Betriebliche Notwendigkeiten (z. B. eine Vertretung) können dazu führen, dass andere Ihr Passwort kennen. [3]Die daraus erwachsenden Gefährdungen lassen sich durch häufigen Passwortwechsel minimieren. [4]Nutzen Sie auch die system- bzw. programmseitigen Möglichkeiten, einen Passwortwechsel zu bestimmten Zeitabständen zu fordern.
☝ Verändern Sie herstellerseitig eingestellte Passwörter!	[1]Herstellerseitig eingestellte Passwörter sind meist allgemein bekannt. [2]Wer diese nicht ändert, arbeitet faktisch mit einem PC ohne Passwortschutz.
☝ Hinterlegen Sie Passwörter an einer sicheren Stelle, damit sie im Bedarfsfall zugänglich sind!	[1]Passwörter sind, z. B. für die Vertretungsregelung, an einem sicheren Ort, z. B. durch versiegelte Aufbewahrung in einem verschlossenen Behältnis, aufzubewahren. [2]Bei jedem Passwortwechsel ist die Aktualisierung des hinterlegten Passwortes erforderlich.
☝ Verschließen Sie nicht genutzte Diskettenlaufwerke mit einem Diskettenschloss (sog. „Maulsperre“)!	Nicht verschlossene Diskettenlaufwerke können zur Umgehung von Schutzmechanismen (z. B.: Bildschirmsperre, Passwortschutz) genutzt werden.
☝ Schützen Sie Schlüssel vor dem Zugriff durch Unbefugte!	[1]Die Schutzwirkung von Disketten-, Tastatur- oder Türschlössern hängt direkt von der sicheren Aufbewahrung der zugehörigen Schlüssel ab. [2]Der Schlüssel vom Diskettenschloss gehört nicht in den unverschlossenen Schreibtisch, der Zimmerschlüssel nicht auf den Flurschrank neben der Tür.

Mögliche Maßnahmen:	Erläuterung:
☞ Aktivieren Sie produktspezifische Sicherheitsfunktionen bedarfsgerecht!	Jede zusätzliche Schutzfunktion (z. B. physikalisches Löschen oder Verschlüsselung), die Ihnen von Ihrem PC oder der Software angeboten wird, kann den Zugriff Unbefugter erschweren und sollte daher genutzt werden.

4. Schützen Sie Programme und Daten vor dem Zugriff durch Unbefugte!

Begründung:

[1]Personenbezogene Daten dürfen aus Gründen des Datenschutzes keinem Dritten zugänglich gemacht werden. [2]Dies gilt auch für Mitarbeiterinnen und Mitarbeiter, die nicht dienstlich mit den von Ihnen zu bearbeitenden Daten befasst sind.

Mögliche Maßnahmen:	Erläuterung:
☞ [1]Beschränken Sie die Art des Zugriffs auf Dateien (z. B. nur Lesen, nicht Schreiben) sowie die Ausführung von Programmen auf befugte Personen. [2]Nutzen Sie dazu Ihre Möglichkeiten der Rechtevergabe. [3]Vergeben Sie die Zugriffe nur für den erforderlichen Zeitraum!	[1]Die Beschränkung von Zugriffsmöglichkeiten, z. B. mittels eines PC-Sicherheitsproduktes, kann Schäden begrenzen, die entstehen können, wenn sich Unberechtigte böswillig Zugang zum System verschafft haben, oder wenn Berechtigte fehlerhafte Aktionen ausführen. [2]Die unkontrollierte Ausbreitung manipulierter Software kann so zwar nicht verhindert, aber deutlich begrenzt werden.
☞ Löschen Sie nicht mehr benötigte Daten möglichst physikalisch!	Auf physikalisch gelöschte Daten ist, unabhängig von erteilten Rechten, kein Zugriff möglich.
☞ Achten Sie darauf, dass Ausdrucke mit personenbezogenen Daten nicht in unbefugte Hände gelangen!	[1]Frei zugängliche Ausdrucke können von Unbefugten gelesen werden. [2]Schließen Sie Ausdrucke mit sensiblem Inhalt ein. [3]Wer Anzahl und Verbleib von Ausdrucken kontrolliert und unnötige Ausdrucke sachgerecht vernichtet (z. B. über den Reißwolf), vermindert die Gefahr der Kenntnisnahme durch Unbefugte.

Mögliche Maßnahmen:	Erläuterung:
☝ Bitte holen Sie Ausdrucke mit personenbezogenen Daten über frei zugängliche Zentraldrucker sofort ab!	Wenn der Zentraldrucker eines Netzwerkes nicht beobachtet wird und Ausdrucke durch Sie nicht sofort abgeholt werden, können Unbefugte die Ausdrucke lesen bzw. entwenden.
☝ Schauen Sie regelmäßig in Info- bzw. Protokolldateien, in denen Zugriffe, Zugriffsversuche, Änderungen an Dateien etc. dokumentiert werden!	[1]In Infodateien (z. B. unter WINWORD „Datei" – „Datei-Info …") werden Angaben über die letzte Änderung, den letzten Ausdruck etc. gespeichert. [2]In Protokolldateien werden Zugriffe über eine bestimmte Zeit hinweg dokumentiert. [3]Sind in einer solchen Datei unplausible Informationen (z. B.: Ausdruck während Abwesenheit) oder unzulässige bzw. abgewiesene Zugriffsversuche im Protokoll enthalten, deutet dies auf den Versuch einer unbefugten Nutzung des PC oder von Daten und Programmen hin.
☝ Nutzen Sie bei der Speicherung vertraulicher Daten und Programme ggf. Verschlüsselungstechniken!	[1]Viele Schutzmechanismen haben eine für den normalen Schutzbedarf ausreichende Qualität. [2]Wird beabsichtigt, sensible Daten zusätzlich zu schützen, kann dies durch eine geeignete Verschlüsselung, z. B. durch ein spezielles Verschlüsselungsprogramm oder durch eine in einem PC-Sicherheitsprodukt integrierte Verschlüsselungsroutine, geschehen.

5. Verhindern Sie die Beschädigung und den Diebstahl von beweglichen Datenträgern (Disketten, Bandkassetten und herausnehmbaren Festplatten)!

Vorbemerkung zu nachfolgenden Sicherheitshinweisen:

[1]Diese Sicherheitstipps gelten nur für PC, die über ein offenes Diskettenlaufwerk, eine herausnehmbare Festplatte oder ein Streamer-Laufwerk für Datensicherungen verfügen. [2]Soweit die PC in einem Netzwerk eingesetzt werden, erfolgt die Datensicherung über den Server zu vorher festgelegten Zeiten automatisch. [3]Offene Diskettenlaufwerke sollten nur an wenigen, besonders geschützten PC-Arbeitsplätzen eingesetzt werden.

Mögliche Maßnahmen:	Erläuterung:
☞ Beschriften Sie Datenträger eindeutig und für autorisierte Benutzer aussagekräftig!	[1]Da Datenträger nicht ohne weiteres unterschieden werden können, ist eine eindeutige Beschriftung von Datenträgern Voraussetzung für deren sichere Handhabung. [2]Das Etikett sollte den Datenträger eindeutig kennzeichnen. [3]Bei Sicherungsdatenträgern sollte zusätzlich das Datum der Sicherung vermerkt sein.
☞ [1]Schließen Sie Disketten, Bandkassetten und herausnehmbare Festplatten, die Sie vorübergehend nicht verwenden, ein. [2]Wenn Sie Datenträger auf Dauer nicht mehr benötigen, geben Sie diese an die DV-Benutzerbetreuung zurück oder deponieren Sie diese in einem Archiv!	[1]Frei zugängliche Datenträger sind nicht gegen Beschädigung oder Entwendung geschützt. [2]Durch Verschluss in einem sicheren Behältnis am Arbeitsplatz wird ein Mindestschutz erreicht. [3]In einem Archiv sind Datenträger deutlich besser gegen Diebstahl oder Beschädigung geschützt.
☞ Achten Sie auf Disketten, Bandkassetten und herausnehmbare Festplatten (Wechselplatten) während der Arbeit!	Durch ihre geringe Größe sind die beweglichen Datenträger (insbesondere Disketten) leicht zu entwenden.
☞ Schützen Sie Datenträger vor Hitze, Schmutz und Flüssigkeiten wie Getränken, Blumenwasser und Chemikalien!	[1]Datenträger sind besonders empfindlich gegen Feuchtigkeit, Verschmutzung und Chemikalien. [2]Derartige Einwirkungen können den Verlust von Daten oder sogar die völlige Unbrauchbarkeit der Disketten zur Folge haben. [3]Verschmutzte oder durch Hitze verformte Disketten können zudem zu Beschädigungen am Laufwerk führen.
☞ Halten Sie Datenträger von magnetischen Feldern wie Bildschirm und elektrischen Geräten fern!	[1]Informationen auf magnetischen Datenträgern können leicht durch magnetische Felder geschädigt werden. [2]Sie sind dann nicht mehr nutzbar.
☞ Führen Sie regelmäßige Bestandskontrollen durch!	Durch Bestandskontrollen lässt sich feststellen, ob Datenträger fehlen oder falsche vorhanden sind.

Mögliche Maßnahmen:	Erläuterung:
☝ Nehmen Sie keine Disketten mit nach Hause!	Es besteht die Gefahr, dass Familienangehörige und weitere Personen die personenbezogenen Daten zur Kenntnis nehmen, kopieren oder an Dritte weitergeben.

6. Schützen Sie Programme und Daten vor einer unbeabsichtigten Zerstörung!

Vorbemerkung zu nachfolgenden Sicherheitshinweisen:

[1]Diese Sicherheitstipps gelten nur für PC, die über ein offenes Diskettenlaufwerk verfügen. [2]Bei PC-Arbeitsplätzen – ohne offene Diskettenlaufwerke – in einem Netzwerk werden über den Server regelmäßig Datensicherungen vorgenommen. [3]Die DV-Benutzerbetreuung ist vor der Installation von Programmen verpflichtet, gemeinsam mit den Fachabteilungen die Zugriffsberechtigungen (Lese-, Schreib- und Druckzugriffe) zu regeln und Programme sowie Fremddaten auf Virenbefall zu prüfen.

Mögliche Maßnahmen:	Erläuterung:
☝ Lösen Sie während der Verarbeitung von Daten keinen erneuten Systemstart aus, z. B. durch den „Reset“-Knopf oder eine gleichbedeutende Tastenkombination („CTRL ALT DEL“ oder „STRG ENTF ALT“.)	[1]Durch den Systemstart während eines Programmlaufes können im Speicher des Rechners enthaltene Daten verloren gehen. [2]Die Vollständigkeit und Korrektheit der Daten ist gefährdet.
☝ Lassen Sie Datenträger nur solange im Laufwerk wie nötig und aktivieren Sie den mechanischen Schreibschutz von Disketten, wenn Sie diese nicht beschreiben müssen (z. B. bei Programmdisketten oder Datensicherungen)!	Durch das Entfernen von Datenträgern aus dem Laufwerk und den mechanischen Schreibschutz kann verhindert werden, dass Daten unbeabsichtigt gelöscht oder überschrieben werden.
☝ Gestatten Sie Zugriffsberechtigungen auf Programme und Daten nur, wenn dies über dienstliche Notwendigkeiten begründet werden kann!	Wenn man die Zugriffsmöglichkeiten beschränkt, kann der Schaden begrenzt werden, wenn Unbefugte mit böswilliger Absicht Zugang zum System gefunden haben oder wenn fehlerhafte Aktionen ausgeführt werden.

Mögliche Maßnahmen:	Erläuterung:
☞ Vergeben Sie besondere Zugriffsberechtigungen (z. B.: „nur Lesen“) für Programme und Daten!	[1]Die Einschränkung der Zugriffsberechtigung auf „nur Lesen“ verhindert das versehentliche Löschen oder Überschreiben von Dateien und Programmen auf der Festplatte. [2]Ein vorsätzliches Löschen oder Überschreiben wird erschwert.
☞ Kopieren Sie den Inhalt von Datenträgern sorgfältig mindestens einmal im Jahr um!	Nach längerer Aufbewahrung ist – wegen der schleichenden Entmagnetisierung – nicht mehr gewährleistet, dass die Informationen auf Datenträgern noch einwandfrei lesbar sind.
☞ [1]Prüfen Sie jede Diskette und CD vor ihrem Einsatz auf Virenfreiheit mit einem geeigneten, aktuellen Viren-Suchprogramm. [2]Die (lokale) Festplatte ist ebenfalls regelmäßig auf Viren zu untersuchen!	[1]Selbst auf Original-Installationsdisketten renommierter Softwarehersteller können sich Viren befinden. [2]Die Schadenswirkung eines Virus kann bis zur Löschung der gesamten Festplatte und somit zum Verlust aller Daten und Programme führen.

7. Benutzen Sie im Dienst keine private Hard- und Software und die dienstliche Hard- und Software nur am Arbeitsplatz!

Vorbemerkung zu nachfolgenden Sicherheitshinweisen:

Ein großer Teil der Sicherheitstipps ist von Ihnen nur zu beachten, wenn an Ihrem Arbeitsplatz ein PC mit offenem Diskettenlaufwerk installiert wurde.

Mögliche Maßnahmen:	Erläuterung:
☞ Benutzen Sie nur dienstlich freigegebene Rechner, Datenträger und Programme!	[1]Durch den Einsatz fehlerhafter oder manipulierter Hard- oder Software ist die Integrität der Programme und Daten, die Verfügbarkeit des Rechners und der Daten sowie deren Vertraulichkeit bedroht. [2]Bei Netzanschluss des Rechners oder wenn mit dem PC mittels Modem Datenfernübertragungen über Leitungen oder Telefon möglich sind, können sich diese Bedrohungen auch auf das Netz und andere angeschlossene PC erstrecken.

Mögliche Maßnahmen:	Erläuterung:
☝ Machen Sie keine unerlaubten Kopien von Programmen und Daten!	[1]„Raubkopien“ verletzen gesetzliche und vertragliche Vorschriften. [2]Beachten Sie in diesem Zusammenhang das Rundschreiben-Nr. 15 des Landeskirchenamtes der EKvW vom 18.08.1997 zum urheberrechtlichen Schutz von Computerprogrammen (Az.: A 14 – 03/01.09).
☝ Spielen Sie keine fremden oder privaten Programme und Daten ein!	[1]Gerade der Einsatz von Software unbekannter oder zweifelhafter Herkunft birgt die Gefahr, dass es zu gefährlichen Veränderungen an Programmen und Daten durch Computerviren oder andere Programme mit Schadenswirkung kommt. [2]Beachten Sie in diesem Zusammenhang das Rundschreiben-Nr. 15 des Landeskirchenamtes der EKvW vom 18.08.1997 zum urheberrechtlichen Schutz von Computerprogrammen (Az.: A 14 – 03/01.09).
☝ [1]Benutzen Sie dienstliche Hardware, Datenträger und Software nur am Arbeitsplatz bzw. nur zu dienstlichen Zwecken (z. B. Laptops). [2]Private Hard- und Software darf nicht am Arbeitsplatz eingesetzt werden!	[1]Durch die Benutzung von Rechnern und Datenträgern andernorts verlieren ortsgebundene Schutzmechanismen (Verschluss, Zutrittskontrollen o. Ä.) ihre Wirkung. [2]Vorhandene Schutzmechanismen sind in der Regel auf die dienstliche Hard- und Software sowie deren Einsatzumgebung abgestimmt. [3]Beim Einsatz privater Geräte und Programme ist der Schutz folglich nicht in gleichem Maße zu gewährleisten. [4]Auch vermeiden Sie dadurch eine finanzielle Haftung Ihrerseits.

8. Löschen Sie Daten immer durch vollständiges Überschreiben!

Vorbemerkung zu nachfolgenden Sicherheitshinweisen:

[1]Diese Sicherheitstipps gelten nur für PC, die über ein offenes Diskettenlaufwerk verfügen. [2]Soweit der PC in einem Netzwerk eingesetzt wird, erfolgt die Löschung der Daten auf der Festplatte des Servers; ein entsprechender Zugangsschutz sollte realisiert sein.

Mögliche Maßnahmen:	Erläuterung:
☞ Löschen Sie alle nicht benötigten Dateien und Programme!	Die Übersicht über Programme und Daten wird erleichtert, wenn nur das erforderliche Minimum gespeichert wird.
☞ Löschen Sie Dateien mit sensiblen personenbezogenen Daten auf Datenträgern (Disketten, Festplatten und Bandkassetten) möglichst immer durch vollständiges Überschreiben der zu löschenden Datei!	[1]Durch Löschfunktionen wie „Delete“ bzw. „Entfernen“ wird lediglich der Speicherbereich freigegeben, eine tatsächliche Löschung von Daten erfolgt dadurch nicht. [2]Derart „pseudogelöschte“ Dateien lassen sich mit handelsüblichen Programmen problemlos wiederherstellen. [3]Die Vertraulichkeit solcher vermeintlich vernichteten Informationen ist besonders dann gefährdet, wenn Datenträger die kontrollierte Umgebung verlassen. [1]Die Funktion „physikalisches Löschen“ wird als Zusatz bei einigen Programmen und Sicherheitsprodukten angeboten. [2]Sie muss in der Regel durch den Benutzer aktiviert werden.
☞ Lassen Sie unbrauchbare oder auszusondernde Datenträger ggf. durch mechanische oder andere physikalische Zerstörung vernichten!	Nur eine vollständige mechanische Zerstörung von Datenträgern bietet die Gewähr, dass Daten nicht mehr rekonstruiert werden können.

9. Schützen Sie Programme und Daten auf allen Kommunikationswegen!

Begründung:

Damit personenbezogene Daten nicht in die Hände von Unbefugten gelangen können, ist für einen geregelten und kontrollierten Datenaustausch zu sorgen.

9.1. PC mit offenem Laufwerk

Soweit Ihr PC über ein offenes Disketten- oder Streamer-Laufwerk verfügt, beachten Sie für den Datenaustausch auf Datenträgern (z. B.: Disketten, DAT-Bändern, Streamern etc.) folgende Sicherheitsregeln:

Mögliche Maßnahmen:	Erläuterung:
☞ Nutzen Sie ggf. die Möglichkeit der Verschlüsselung der Daten. Ist dies nicht möglich, sollten die Datenträger zumindest über sichere Kanäle (z. B. Boten) verschickt werden.	Werden Datenträger mit unverschlüsselten Daten verschickt, können diese Daten Unbefugten zur Kenntnis gelangen

9.2 PC mit Möglichkeiten zur Datenfernübertragung (Modem)

Soweit Sie mit dem PC beispielsweise mit Hilfe eines Modems über Telefonleitungen Verbindungen zu anderen Dienststellen oder Institutionen aufnehmen können, beachten Sie für einen Daten- und Programmaustausch folgende Sicherheitsregeln:

Mögliche Maßnahmen:	Erläuterung:
☞ Stellen Sie durch korrekte Eingabe und Prüfung der Adressinformationen die richtige Verbindung zum beabsichtigten Empfänger sicher!	Wenn Daten nicht an den beabsichtigten Empfänger, sondern an einen falschen gesandt werden, kann die Vertraulichkeit von Daten verletzt werden.
☞ Benutzen Sie nach Möglichkeit nur gesicherte Leitungen und nutzen Sie insbesondere bei sensiblen personenbezogenen Daten die Möglichkeit der Verschlüsselung bei der Übertragung auf ungesicherten Verbindungswegen, wie öffentlichen Netzen!	[1]Leitungen, die nicht gegen Abhören, Beschädigung oder Unterbrechung gesichert sind, stellen Bedrohungen für die Vertraulichkeit, Integrität und Verfügbarkeit von Daten dar. [2]Die Kenntnisnahme von Daten durch Unbefugte mittels Abhören lässt sich nur durch Nutzung von entsprechend gesicherten Leitungen oder eine geeignete Verschlüsselung verhindern.

10. Informieren Sie immer die systembetreuende Stelle, ggf. auch die Betriebsbeauftragte oder den Betriebsbeauftragten für den Datenschutz bzw. die Ansprechpartnerin- bzw. den Ansprechpartner in Datenschutzfragen und ggf. die Vorgesetzten über ungewöhnliche Ereignisse!

Begründung:

[1]Ein verändertes Programm- und Systemverhalten kann ein Hinweis auf unberechtigte Hard- oder Softwareveränderungen sein. [2]Indem Mitteilungen über ungewöhnliche Ereignisse frühzeitig weitergegeben werden, kann die Begrenzung und Behebung eines Schadens entscheidend erleichtert werden.

Mögliche Maßnahmen:	Erläuterung:
☝ Beginnen Sie die Arbeit am PC grundsätzlich mit dem Einschalten des Bildschirms und achten Sie auf verändertes Programm- und Systemverhalten beim Beginn und während der Arbeit!	[1]Beim Hochfahren des PC erscheint eine Reihe von Meldungen auf dem Bildschirm. [2]Durch aufmerksames Betrachten können veränderte oder fehlende Meldungen festgestellt werden. [3]Dies kann auf eine Veränderung in der Hard- oder Software des PC oder einen Virenbefall hindeuten.
☝ Informieren Sie die systembetreuende Stelle, ggf. auch die Betriebsbeauftragte oder den Betriebsbeauftragten für den Datenschutz bzw. die Ansprechpartnerin bzw. den Ansprechpartner in Datenschutzfragen und ggf. die Vorgesetzten über unerwartetes Verhalten und über ungewöhnliche Ereignisse. Teilen Sie den o. a. Personen mit, wenn sich einer dieser 10 Tipps nicht umsetzen lässt!	Das Wissen und die Erfahrung der mit dem Datenschutz betrauten Personen und der Systembetreuung sollen den PC-Benutzern im Zweifels- und Schadensfall helfen, die Situation einzuschätzen und ggf. zu bereinigen, denn nicht alle PC-Benutzer verfügen über sicherheitstechnische Spezialkenntnisse.
☝ Fragen Sie bei der systembetreuenden Stelle, ggf. auch bei der oder dem Betriebsbeauftragten für den Datenschutz bzw. der Ansprechpartnerin oder dem Ansprechpartner in Datenschutzfragen nach, wenn einzelne vorgenannte Maßnahmen nicht umgesetzt sind.	[1]Zum Teil sind aus Unkenntnis nicht alle möglichen Datensicherungs- und Datenschutzmaßnahmen umgesetzt. [2]Um eine möglichst optimale Schutzwirkung zu erreichen, sind die betroffenen Stellen auch von Anwenderseite zu sensibilisieren. [3]Die Entscheidung darüber, inwieweit wünschenswerte Sicherheitsmaßnahmen notwendig sind und umgesetzt werden, liegt bei der Leitung der kirchlichen Körperschaft.

Passwörter für DV-Anwendungen und Datenschutz

Merkblatt der Evangelischen Kirche von Westfalen zur datenschutzgerechten Gestaltung von Passwörtern

– Stand 01.03.1999 –

These 1:	These 2:
Leicht zu merkende Passwörter sind leicht zu erraten.	Schwer zu merkende Passwörter werden oft aufgeschrieben.
B e i d e s i s t s c h l e c h t !	

Ein Passwort sollte folgenden Forderungen genügen:

- Ein Passwort muss mindestens 6 Zeichen lang sein!
- Ein Passwort sollte aus einer Kombination von Buchstaben und Zahlen oder Sonderzeichen gebildet werden.
- [1]Das System, das die Passwörter abfragt und prüft, sollte möglichst zwischen Groß- und Kleinschreibung unterscheiden können. [2]Die Verwendung beliebiger Tastaturzeichen sollte zulässig sein.Die Verwendung beliebiger Tastaturzeichen sollte zulässig sein.

Beispiel zur Passwortbildung

- Ein Passwort sollte aus zwei voneinander unabhängigen Wörtern oder einer Redewendung bestehen, z. B.: „Nebel“ und „Baum“ bzw. „Ex und Hopp“.
- Die zusammengesetzten Wörter bzw. die Redewendung sind so zu kürzen, dass sie die zulässige Länge haben, z. B.: „NEBEBAUM“ bzw. „EXUNDHOP“.
- Ein Zeichen der so entstandenen Zeichenfolge wird durch ein Sonderzeichen ersetzt, z. B.: „NEB§BAUM“, oder die Zeichenfolge wird durch einen oder mehrere Schreibfehler verändert, z. B.: „EXUNT-HOB“:

Beispiel zum Passwortwechsel

- Passwörter sind regelmäßig zu wechseln.
- Der Passwortwechsel sollte system- bzw. programmseitig nach Ablauf einer voreingestellten Zeit verlangt werden.
- Um zu verhindern, dass der Anwender das gleiche Passwort beim Wechsel direkt wieder einstellt, oder system- bzw. programmseitig zwei Passwörter im Wechsel nutzt, ist eine Passworthistorie mindestens über die letzten 4 benutzten Passwörter zu führen.
- [1]System- oder programmseitig (ggf. über eine zusätzlich installierte Sicherheitssoftware) sollten möglichst Trivialpasswörter erkannt und abgelehnt werden. [2]Die Liste von Trivialpasswörtern sollte durch den Anwender ergänzt werden.

Computerviren und Datenschutz

Merkblatt der Evangelischen Kirche von Westfalen zum Datenschutz und zur Datensicherheit betreffend Computerviren[1]

– Stand 01.03.1999 –

Allgemeines

[1]Computerviren sind Programme mit Schadensfunktion, die zur Verfälschung oder zum Verlust von Daten (bis zur Löschung der gesamten Festplatte) führen können. [2]Computerviren gelangen als Teil eines Programms oder einer Datei in den PC. [3]Wenn ein derart infiziertes Programm aufgerufen oder eine infizierte Datei bearbeitet wird, dann aktiviert dieses auch den Virus. [4]Neben seiner direkten Schadensfunktion auf Daten hat ein Computervirus die Eigenschaft, sich selbstständig in andere Dateien (Programme und Daten) hinein zu kopieren. [5]Dadurch kommt es zu einer unkontrollierten Ausbreitung eines Virus im PC.

[1]Computerviren werden meistens beim Datenaustausch per Diskette oder über ein Netzwerk (z. B. per E-Mail) übertragen. [2]Es wird aber auch von Fällen berichtet, bei denen schon auf den Original-Programm-Disketten oder -CD renommierter Softwarehersteller Viren gefunden worden sind.

Was deutet auf einen Virenbefall hin?

[1]In den meisten Fällen wird ein Virus erst anhand seiner Auswirkungen und Schäden erkannt. [2]Dazu gehören u.a.:

- Unnormales Verhalten des PC
- Unerwartete Verzögerungen beim Aufruf von Programmen und Daten
- Unerklärlicher Rückgang des verfügbaren Speicherplatzes im Arbeitsspeicher oder auf der Festplatte
- Auffällig lange Reaktionszeiten im Programmablauf
- Unerklärliche Systemabstürze in bisher einwandfrei laufenden Programmen
- Falsche oder veränderte Bildschirmdarstellung
- Veränderte oder fehlende Dateien bzw. Programme

Wie sollte man sich beim Verdacht auf Virenbefall verhalten?

1 Dieses Merkblatt beruht auf Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit Dienstsitz in Bonn, das für die tägliche Arbeit im kirchlichen Bereich entsprechend angepasst wurde.
Informationen und Programme zum Thema Viren und Virensuche können im BSI-Internet-Server unter www.bsi.bund.de abgerufen werden.
Im Übrigen bietet das BSI eine Viren-Hotline an: Tel.: 0228/9582-444, Fax: 0228/9582-427, E-Mail antivir @ bsi.de.

- Informieren Sie sofort die systembetreuende Stelle und stimmen Sie weitere Maßnahmen mit ihr ab.
- Beenden Sie möglichst bald alle Arbeiten am PC wie gewohnt.
- Schalten Sie den PC aus.

Unerfahrene PC-Nutzer sollten auf keinen Fall selber versuchen, die infizierten Dateien und Programme zu suchen und zu löschen.

Wie kann man einem Virenbefall vorbeugen?

Die folgenden vorbeugenden Schutzmaßnahmen sind bei PC mit offenen Diskettenlaufwerken bzw. mit direktem Anschluss per E-Mail oder ans Internet notwendig, um einen Virenbefall zu verhindern:

- Lassen Sie Ihren PC so einstellen, dass er standardmäßig von der Festplatte und nicht von der Diskette startet (bootet)! (erweitertes CMOS:C:, A: statt A:, C:).
- Überprüfen Sie jede Ihnen unbekannte Diskette vor dem ersten Lesezugriff mittels eines aktuellen Viren-Suchprogramms auf Virenbefall.
- Dateien, die über ein Netz in Ihren PC gelangen (z. B.: per E-Mail oder Internet), sind ebenfalls vor dem ersten Zugriff durch ein aktuelles Viren-Suchprogramm zu prüfen.
- Durchsuchen Sie die Festplatte regelmäßig mittels Viren-Suchprogramm nach Viren.
- [1]Immer, wenn Ihnen eine neue Version des Viren-Suchprogramms zur Verfügung steht, sollten Sie die Festplatte und die Datenträger erneut durchsuchen. [2]Dadurch werden ggf. Viren entdeckt, die von der vorherigen Version noch nicht erkannt werden konnten.

Was ist sonst noch zu tun?

- Bei Viren auf Programmdisketten informieren Sie bitte neben der systembetreuenden Stelle den Händler und Programm-Hersteller.
- Bei Datendisketten informieren Sie den Ersteller der Diskette und warnen Sie Benutzer, die infizierte Disketten von Ihnen erhalten haben.