

Richtlinie über die Nutzung des landeskirchlichen Intranets (Intranetrichtlinie)

KABl. 2011 S. 80

Das Landeskirchenamt hat in seiner Sitzung am 8. Februar 2011 gem. § 6 Verordnung über die Intranet- und Internetnutzung in der Evangelischen Kirche von Kurhessen-Waldeck vom 12. November 2010 die folgende Richtlinie beschlossen:

§ 1 Anwendungsbereich

1Kernelement der Informationstechnologie (IT) ist die Gewährleistung von Datenverarbeitung und -übermittlung sowie die Bereitstellung von Informationen. 2Bestandteil zur Umsetzung dieser Aufgaben ist der Betrieb eines landeskirchenweiten Intranets (EKKW.intern). 3Die Nutzung des Intranets dient der Bereitstellung und dem Austausch dienstlicher Daten. 4Die Nutzung des integrierten landeskirchlichen E-Mailsystems und der sonstigen sich fortlaufend weiterentwickelnden Arbeitshilfen (Workflows) dienen der dienstlichen Kommunikation. 5Diese Richtlinie gilt für Anwender und Betreuer des Intranets.

§ 2 Zugang zum Intranet

1Der Zugang zum Intranet erfolgt regelmäßig über die dienstlichen, zentral bereit gestellten, Rechner. 2In begründeten Ausnahmefällen ist der Zugang über private Rechner möglich. 3Ein begründeter Ausnahmefall liegt insbesondere vor, wenn ein Zugang über dienstliche Rechner nicht verfügbar ist. 4Die Entscheidung hierüber trifft das zuständige vertretungsberechtigte Organ oder eine von diesem im Rahmen der vorgegebenen Zuständigkeiten beauftragte Stelle. 5Kirchliche Körperschaften, Verwaltungs- und sonstige Stellen, die an das Intranet angeschlossen werden, nutzen die regelmäßig vorhandenen Computernetze um das Intranet zu erreichen.

§ 3 IT-Sicherheit

(1) Sicherheitsziele der IT und des Intranets

1Informations- und Kommunikationssysteme und dienstliche Daten sind vor unberechtigtem Zugriff und vor unerlaubter Änderung zu schützen (IT-Sicherheit). 2Jede kirchliche Körperschaft ist verpflichtet, IT-Sicherheit zu gewährleisten. 3Dafür ist das jeweilige Leitungsorgan verantwortlich.

4Daten und IT-Systeme sind in ihrer Verfügbarkeit so zu sichern, dass die zu erwartenden Stillstandzeiten das laufende Dienstgeschäft nicht beeinträchtigen. 5Fehlfunktionen und

Unregelmäßigkeiten in Daten und IT-Systemen sind zu vermeiden (Integrität). ⁶In den Bereichen, in denen Programme mit schutzbedürftigen Daten eingesetzt werden, insbesondere Meldewesen, Personalwesen, Haushalts-, Kassen- und Rechnungswesen, sind die IT-Sicherheitsziele (Verfügbarkeit, Integrität und Vertraulichkeit) besonders zu beachten.

⁷Im Rahmen dieser Richtlinie und den sonstigen Hinweisen des Landeskirchenamtes ist jede kirchliche Körperschaft verpflichtet, zur Erreichung dieser IT-Sicherheitsziele, IT-Sicherheit zu beachten.

(2) IT- Sicherheitsmaßnahmen

¹Zur Umsetzung der IT-Sicherheit sind die Vorgaben des Landeskirchenamtes zu beachten. ²Hierfür wird vom Landeskirchenamt ein IT-Sicherheitskonzept erstellt, das Bestandteil des Handbuchs (§ 6) ist. ³Die im IT-Sicherheitskonzept definierten Sicherheitsmaßnahmen müssen umgesetzt werden. ⁴Diese Umsetzung kann durch das Landeskirchenamt oder eine von ihr beauftragte Stelle überprüft werden. ⁵Die IT-Sicherheitsmaßnahmen sollen in einem angemessenen Verhältnis zum Wert der schützenswerten Daten und IT-Systeme stehen.

⁶IT-Benutzer und sonstige beteiligte Personen und Stellen sind für die Einhaltung des für die jeweilige kirchliche Körperschaft oder Untergliederung geltenden IT-Sicherheitskonzeptes verantwortlich. ⁷Wenn dienstliche Daten an außerkirchliche Stellen, die nicht in EKKW.intern eingebunden sind, weitergeleitet werden müssen, ist eine größtmögliche Datensicherheit zu gewährleisten. ⁸Sollte ein Sicherheitsproblem bestehen, ist dem IT-Verantwortlichen unverzüglich der entsprechende Warnhinweis zu melden. ⁹Maßnahmen sollen erst nach Rücksprache mit dem IT-Verantwortlichen umgesetzt werden.

(3) Schutzmaßnahmen

¹Kirchliche Stellen haben dafür zu sorgen, dass ihr internes Netz durch eine geeignete Firewall gesichert wird. ²Dies wird im Bereich der Pfarrämter zentral durch die Landeskirche geregelt und bereit gestellt.

³Jeder Rechner benötigt einen aktuellen und aktivierten Schutz vor Schadsoftware. ⁴Ein Virenschutzprogramm mit aktuellen Signatur-Dateien ist zu installieren. ⁵Die Signatur-Dateien müssen durch Updates regelmäßig aktualisiert werden. ⁶Für dienstliche Rechner ist ein einheitliches Virenschutzprogramm zu verwenden, welches durch das Landeskirchenamt festgelegt wird.

⁷Aktualisierungen von Betriebssystemen und einzelne Anwendungsprogramme wie z.B. der Internet-Browser sollen ohne zeitliche Verzögerung nach Freigabe durch das Landeskirchenamt installiert werden.

⁸Dienstliche Daten sind in geschützten Bereichen zu speichern. ⁹Dabei sind die datenschutzrechtlichen Vorgaben einzuhalten. ¹⁰Der Zugang zu zentralen Servern und Netzwerkkomponenten soll durch ausreichende Zugangskontrollen geschützt werden. ¹¹Der

Zugang zu IT-Systemen soll durch angemessene Zugangskontrollen, der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt werden.

¹²Vor Ort sind Regelungen für eine angemessene Datensicherung und Maßnahmen zur Notfallvorsorge zu treffen. ¹³IT-Benutzer haben bei Störfällen die zuständige Stelle zu benachrichtigen. ¹⁴Darüber hinaus werden IT-Benutzer regelmäßig über die Gefahren im Umgang mit IT informiert; entsprechende Informationen und Hinweise finden sich bedarfsweise aktualisiert im Intranetportal der Landeskirche.

(4) Dokumentation

¹Für das Intranet der Landeskirche und diesem angeschlossene Rechner werden zur Sicherheit und Kontrolle der Daten entsprechende Protokolle auf den Servern der Netzknotenpunkte erstellt. ²Die Protokolle werden mindestens für die Dauer eines halben Jahres aufbewahrt. ³Längere gesetzliche Aufbewahrungspflichten bleiben unberührt.

§ 4 E-Mail Nutzung

¹Die Nutzung von E-Mails wird in einer Rundverfügung und im Handbuch gem. § 6 geregelt. ²Für die elektronische Kommunikation mittels E-Mails gelten die Vorschriften über die Einhaltung des Dienstwegs entsprechend.

§ 5 Internetnutzung

¹Downloads von Programmen und Dateien außerhalb des dienstlichen Kontextes ist mit dienstlichen Geräten untersagt. ²Jede Datei ist grundsätzlich mit einem aktuellen Virenschutzprogramm zu überprüfen.

§ 6 Handbuch

¹Weitere Handlungsvorgaben und Empfehlungen werden als Anlage zu dieser Richtlinie in Form eines Handbuches geregelt. ²Das Handbuch wird vom Landeskirchenamt in digitaler Form herausgegeben, im Intranet veröffentlicht und regelmäßig aktualisiert.

§ 7 Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung im kirchlichen Amtsblatt in Kraft.

