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

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

§ 2 Zugang zum Intranet

[1]Der Zugang zum Intranet erfolgt regelmäßig über die dienstlichen, zentral bereit gestellten, Rechner. [2]In begründeten Ausnahmefällen ist der Zugang über private Rechner möglich. [3]Ein begründeter Ausnahmefall liegt insbesondere vor, wenn ein Zugang über dienstliche Rechner nicht verfügbar ist. [4]Die Entscheidung hierüber trifft das zuständige vertretungsberechtigte Organ oder eine von diesem im Rahmen der vorgegebenen Zuständigkeiten beauftragte Stelle. [5]Kirchliche 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

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

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

Unregelmäßigkeiten in Daten und IT-Systemen sind zu vermeiden (Integrität). [6]In 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.

[7]Im 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

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

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

(3) Schutzmaßnahmen

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

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

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

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

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

[12]Vor Ort sind Regelungen für eine angemessene Datensicherung und Maßnahmen zur Notfallvorsorge zu treffen. [13]IT-Benutzer haben bei Störfällen die zuständige Stelle zu benachrichtigen. [14]Darüber 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

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

§ 4 E-Mail Nutzung

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

§ 5 Internetnutzung

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

§ 6 Handbuch

[1]Weitere Handlungsvorgaben und Empfehlungen werden als Anlage zu dieser Richtlinie in Form eines Handbuches geregelt. [2]Das 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.