Ev. Kirchenkreis Recklinghausen

Evangelischer Kirchenkreis
Gladbeck · Bottrop · Dorsten

IT-Sicherheitsrichtlinie

Der Kreissynodalvorstand verabschiedet hiermit folgende, aktualisierte Leitlinie zur Informationssicherheit als Bestandteil ihrer Strategie:

Bedeutung der Informationstechnologie (IT)
Informationstechnologie ist ein Instrument zur Erfüllung von wichtigen Aufgaben und zur Unterstützung von Funktionen auf allen Ebenen der Evangelischen Kirche von Westfalen. IT-Systeme und dienstliche Daten sind vor unberechtigtem Zugriff und vor unerlaubter Änderung zu schützen (IT-Sicherheit). Jede kirchliche Körperschaft ist verpflichtet, IT-Sicherheit zu gewährleisten. Dafür ist das jeweilige Leitungsorgan verantwortlich.

Unabhängig von dieser Verantwortlichkeit unterstützen Pfarrerinnen und Pfarrer, Presbyterinnen und Presbyter und Mitarbeitende der kirchlichen Körperschaften die IT-Sicherheit im Rahmen ihrer Tätigkeit.

IT-Sicherheitsziele
Die Daten und IT-Systeme werden in ihrer *Verfügbarkeit* so gesichert, dass die zu erwartenden Ausfallszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (*Integrität*). Die Anforderungen an *Vertraulichkeit* haben ein normales, an Gesetzeskonformität orientiertes Niveau. Zur Erreichung dieser IT-Sicherheitsziele ist jede kirchliche Körperschaft verpflichtet, IT-Sicherheit zu organisieren.

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

Die Nutzung des landeskirchlichen Intranets (Kirchliches Netz Westfalen – KiNet-W) dient zur Bereitstellung und zum Austausch dienstlicher Daten. Die Nutzung des landeskirchlichen E-Mailsystems dient zur dienstlichen Kommunikation. Entsprechende Maßnahmen stellen sicher, dass die Risiken gering bleiben.

Die gesetzlichen Regelungen sind zu beachten. Materielle und immaterielle Folgen durch Gesetzesverstöße, sowie die Verursachung sonstiger Schäden, müssen verhindert werden.

IT-Sicherheitsmanagement
Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet. Es ist ein IT-Sicherheitsbeauftragter benannt worden. Der IT-Sicherheitsbeauftragte berichtet in seiner Funktion direkt der jeweiligen Leitung.
Eine Vertretung der IT-Sicherheitsbeauftragten Person, sowie die Dokumentation zur Systemadministration und zum Berechtigungsmanagement wurde sichergestellt.

IT- Sicherheitsmaßnahmen

Zur Umsetzung der IT-Sicherheit wurde ein IT-Sicherheitskonzept erstellt. Das IT-Sicherheitskonzept enthält geeignete Maßnahmen gegen Gefährdungen von innen und außen.
Die IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Wert der schützenswerten Daten und IT-Systeme stehen. Die im IT-Sicherheitskonzept definierten Sicherheitsmaßnahmen, insbesondere Maßnahmen gegen die Bedrohungen von innen und außen, müssen umgesetzt werden. Diese Umsetzung wird regelmäßig in Form von Audits überprüft.

Der Zugang zu KiNet-W für den dienstlichen Gebrauch kann auch über private Rechner erfolgen. Beim Zugang zu KiNet-W über private Rechner ist durch Vereinbarung insbesondere Folgendes zu regeln:

- geeignete Maßnahmen gegen Gefährdungen von innen und außen,
- Anwendung des kirchlichen Datenschutzrechtes,
- technische und organisatorische Maßnahmen zur Datensicherheit und zum Datenschutz.

Sonstige von einer kirchlichen Körperschaft beauftragte Stellen, die im Interesse der kirchlichen Arbeit einen Zugang zu KiNet-W benötigen, können zugelassen werden. Diese Personen und Stellen sind für die Einhaltung des für die jeweilige kirchliche Körperschaft geltenden IT-Sicherheitskonzeptes verantwortlich.

Wenn dienstliche Daten an außerkirchliche Stellen, die nicht in KiNet-W eingebunden sind, weitergeleitet werden müssen, ist eine größtmögliche Datensicherheit zu gewährleisten.

Daneben sind über die Erfordernisse des Datenschutzes hinaus alle dienstlichen Daten in geschützten Bereichen zu speichern.

Der Zugang zu zentralen Servern und Netzwerkkomponenten soll durch ausreichende Zugangskontrollen geschützt werden. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen geschützt. Der Zugriff auf die Daten wird durch ein restriktives Berechtigungskonzept geschützt.

Jede kirchliche Körperschaft sorgt dafür, dass ihr internes Netz durch eine geeignete Firewall gesichert wird. IT-Benutzer informieren bei Störfällen die IT-Sicherheitsbeauftragte Person. IT-Benutzer sollen über die Gefahren im Umgang mit IT regelmäßig informiert werden.
Für eine angemessene Datensicherung müssen Regelungen getroffen werden. Zusätzlich müssen auch Maßnahmen zur Notfallvorsorge getroffen werden.

Zur Erreichung der IT-Sicherheitsziele ist eine regelmäßige Weiterbildung der IT-Sicherheitsbeauftragten Person sowie die Verpflichtung zur Informationsbeschaffung erforderlich.

Gladbeck, 29.10.2018
Ort, Datum

(Siegel)

Der Kreissynodalvorstand:

Superintendent

Mitglied des KSV