

Die Kirchenleitung hat auf ihrer Sitzung am 4. Dezember 2009 folgende Verordnung beschlossen:

**Verordnung
vom 4. Dezember 2009
zur Sicherstellung der Anforderungen an den Datenschutz
in der Informationstechnik (IT)
(IT-Sicherheitsverordnung)**

veröffentlicht im KAbI 2009 S. 154

Die Kirchenleitung hat auf Grund von § 27 Absatz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 12. November 1993 (AbI. EKD 1994 S. 35), geändert durch das Kirchengesetz vom 7. November 2002 (Bekanntmachung in der ab 1. Januar 2003 geltenden Fassung vom 20. Februar 2003 und vom 7. April 2003, AbI. EKD S. 74 und 117) die folgende Verordnung erlassen:

Inhaltsverzeichnis	Seite
§ 1 Geltungsbereich	1
§ 2 IT-Sicherheitsstandard	1
§ 3 IT-Sicherheitsziele	1
§ 4 Zuständigkeit für die Umsetzung der IT-Sicherheitsverordnung	2
§ 5 IT-Sicherheitsbeauftragter	2
§ 6 Kontrolle über die Einhaltung der IT-Sicherheitsverordnung	2
§ 7 Änderung und Aktualisierung der IT-Sicherheitsverordnung	2
§ 8 Sprachliche Gleichstellung	2
§ 9 Durchführungsvorschriften	2
§ 10 Inkrafttreten	3

§ 1

Geltungsbereich

Die IT-Sicherheitsverordnung ist verbindlich für sämtliche Mitarbeitende im Sinne des § 1 Datenschutzverordnung sowie für Dritte, mit denen die Benutzung von Computern und Netzen von kirchlichen und diakonischen Einrichtungen vereinbart worden ist.

§ 2

IT-Sicherheitsstandard

Der Oberkirchenrat und der Vorstand des Diakonischen Werkes werden beauftragt, den gestaffelten IT-Sicherheitsstandard auf Basis des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der Evangelisch-Lutherischen Landeskirche Mecklenburgs und der Diakonie einheitlich festzulegen.

§ 3

IT-Sicherheitsziele

(1) Die IT-Sicherheitsverordnung definiert grundlegende Ziele einer IT-Sicherheit und legt Verantwortlichkeiten sowie Rahmenbedingungen für die Umsetzung des IT-Sicherheitsstandards fest.

(2) Die mit der Informationstechnik erhobenen, verarbeiteten, übertragenen und gespeicherten Daten sind zu schützen, insbesondere im Hinblick auf

1. deren Zugänglichkeit/Verfügbarkeit

Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit bei Bedarf verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren.

2. deren Integrität
Daten und Anwendungen dürfen nicht gelöscht, zerstört oder manipuliert werden.
3. den Schutz der Daten vor Verlust
Der Verlust der Daten ist durch geeignete Maßnahmen zu verhindern.
4. Vertraulichkeit
Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt dem jeweiligen Verfügungsberechtigten.
5. die Einführung, Auswahl, Gestaltung und Änderung von Verfahren
In die Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist der zuständige kirchliche Datenschutzbeauftragte rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.

§ 4

Zuständigkeit für die Umsetzung der IT-Sicherheitsverordnung

Zuständig für die Umsetzung der IT-Sicherheitsverordnung ist im Bereich der Evangelisch-Lutherischen Landeskirche Mecklenburgs der Oberkirchenrat, im Bereich des Diakonischen Werkes der Träger der jeweiligen Einrichtung, soweit nicht im IT-Grundschutz etwas anderes festgelegt wird. Diese Aufgabe kann im Rahmen des Direktionsrechts an den IT-Sicherheitsbeauftragten delegiert werden.

§ 5

IT-Sicherheitsbeauftragter

Der IT-Sicherheitsbeauftragte sowie ein Stellvertreter werden für den Bereich der Evangelisch-Lutherischen Landeskirche Mecklenburgs vom Oberkirchenrat, für den Bereich des Diakonischen Werkes vom Vorstand bestellt. Die Evangelisch-Lutherische Landeskirche Mecklenburgs und das Diakonische Werk können gemeinsam einen IT-Sicherheitsbeauftragten bestellen.

§ 6

Kontrolle über die Einhaltung der IT-Sicherheitsverordnung

Bei Verstößen gegen die IT-Sicherheitsverordnung sind neben den arbeitsrechtlichen und datenschutzrechtlichen folgende Sanktionen möglich:

1. die Beanstandung bei geringfügigen individuellen Verstößen,
2. die Aufforderung an die Leitung der Einrichtung, den Missstand unter Wahrung einer Frist zu beseitigen,
3. bei Zuwiderhandlung oder Nichteinhaltung der Frist nach Nummer 2 die Mitteilung an die Aufsichtsbehörde, im Wege der Aufsicht die Beseitigung des Missstandes anzuordnen,
4. die vorübergehende Sperrung der Zugangsberechtigung zur Datenverarbeitungsanlage bis der Nachweis über die Beseitigung des Missstandes erbracht ist.

§ 7

Änderung und Aktualisierung der IT-Sicherheitsverordnung

Die Kirchenleitung hat die IT-Sicherheitsverordnung in regelmäßigen Abständen zu aktualisieren.

§ 8

Sprachliche Gleichstellung

Soweit in dieser Verordnung Bezeichnungen, die für Frauen und Männer gelten, in der männlichen Sprachform verwendet werden, gelten diese Bezeichnungen für Frauen in der weiblichen Sprachform.

§ 9

Durchführungsvorschriften

Der Oberkirchenrat ist berechtigt, Durchführungsvorschriften zu erlassen.

§ 10
Inkrafttreten

Diese Rechtsverordnung tritt am 1. Januar 2010 in Kraft.

Schwerin, 4. Dezember 2009

Der Vorsitzende der Kirchenleitung

Dr. von Maltzahn
Landesbischof