Erzbischöfliches Ordinariat

Verordnungen

79. IT-Nutzungsrichtlinie für die Informations- und Kommunikationssysteme der Erzdiözese München und Freising

Inhaltsverzeichnis

Präambel

1 Geltungsbereich
- 1.1 Persönlicher Geltungsbereich
- 1.2 Sachlicher Geltungsbereich
- 1.3 Räumlicher Geltungsbereich
- 1.4 Zeitlicher Geltungsbereich
- 1.5 Bestehende Regelungen

2 Inhalt
- 2.1 Allgemeine Nutzungsbedingungen für die Nutzung der IuK-Systeme
- 2.2 Sorgfaltspflichten in Bezug auf den Umgang mit IuK-Systemen
- 2.3 Netzwerkdienste
- 2.4 Elektronische Kommunikation (E-Mail)

3 Inkrafttreten dieser Richtlinie

Präambel

(A) Die elektronischen Informations- und Kommunikationssysteme, diese umfassen die bereitgestellte Hardware, Software und die IT-Dienste, insbesondere Inter- und Intranet sowie E-Mail (im Folgenden „IuK-Systeme“) der Erzdiözese München und Freising KdöR (im Folgenden: „Erzdiözese“ oder „Dienstgeber“) sollen der schnelleren, umfassenden und zeitgemäßen Kommunikation und Information der Mitarbeiterinnen und Mitarbeiter (vgl. Definition in Ziffer 1.1) untereinander sowie zu Einrichtungen und geschäftlichen Kontakten der Erzdiözese dienen.

(B) Gegenstand dieser IT-Nutzungsrichtlinie für die IuK-Systeme der Erzdiözese (im Folgenden: „IT-Nutzungsrichtlinie“) ist die Nutzung der IuK-Systeme durch die Mitarbeiterinnen und Mitarbeiter der Erzdiözese.

(C) Diese IT-Nutzungsrichtlinie dient der Umsetzung von §§ 26 Abs. 1 lit. b), 7 Abs. 2 Gesetz über den Kirchlichen Datenschutz (KDG) i.V.m. §§ 6 und 7 Abs. 1 Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz (KDG-DVO). Die Richtlinie über die Benutzung von Arbeitsplatzcomputern (APC) im Bereich des Erzbischöflichen Ordinariats (Amtsblatt Nr. 9/2001, S. 245 ff.) ist gemäß § 28 Abs. 2 KDG-DVO mit Ablauf des 28. Februar 2019 außer Kraft getreten.

(D) Ebenfalls trägt die IT-Nutzungsrichtlinie dazu bei, die Anforderungen des Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001:2013 im Erzbischöflichen Ordinariat München als Verwaltung der Erzdiözese umzusetzen.

Dies vorausgesetzt wird die folgende IT-Nutzungsrichtlinie erlassen:

1 Geltungsbereich

1.1 Persönlicher Geltungsbereich

In persönlicher Hinsicht gilt diese IT-Nutzungsrichtlinie für alle Kleriker, Beamtinnen und Beamten, Mitarbeiterinnen und Mitarbeiter einschließlich Auszubildenden, Praktikantinnen und Praktikanten (im Folgenden: „Mitarbeiterinnen und Mitarbeiter“) der Erzdiözese, unabhängig von Art und Umfang ihrer Beschäftigung.

1.2 Sachlicher Geltungsbereich

In sachlicher Hinsicht gilt diese IT-Nutzungsrichtlinie für die Nutzung der dienstlichen IuK-Systeme. Sofern seitens des Dienstgebers durch gesonderte Vereinbarung den Mitarbeiterinnen und Mitarbeitern gestattet wird, private Geräte zu dienstlichen Zwecken zu nutzen, oder über private Endgeräte (z. B. PCs, Mobiltelefon, Tablet Computer) auf IuK-Systeme Zugriff zu nehmen, gelten vorbehaltlich etwaiger Regelungen in einer anderen

Richtlinie/Vereinbarung sowie vorbehaltlich der Regelungen in § 20 der Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz (KDG-DVO), die Regelungen dieser IT-Nutzungsrichtlinie entsprechend.

1.3 Räumlicher Geltungsbereich

In räumlicher Hinsicht gilt diese IT-Nutzungsrichtlinie sowohl für alle Dienststellen der Erzdiözese als auch bei Tätigkeiten außerhalb der Dienststellen (z. B. bei Reisetätigkeiten, Außendiensteinsätzen, Telearbeit, mobiles Arbeiten).

1.4 Zeitlicher Geltungsbereich

Der zeitliche Geltungsbereich dieser IT-Nutzungsrichtlinie (Inkrafttreten und Gültigkeit) ist in Ziffer 3 geregelt.

1.5 Bestehende Regelungen

Folgende Regelungen bleiben durch diese IT-Nutzungsrichtlinie unberührt:

(A) Gesetz über den Kirchlichen Datenschutz (KDG) sowie Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz (KDG-DVO),

(B) Regelungen des Arbeitsvertragsrechtes der bayerischen Diözesen (ABD) in ihrer jeweils gültigen Fassung, veröffentlicht unter www.onlineabd.de.

Folgende Vereinbarungen zwischen der Mitarbeitervertretung Erzbischöfliches Ordinariat München und dem Erzbischöflichen Ordinariat München:

(C) Regelungen der Dienstvereinbarung zur Durchführung von Internetstichproben zwischen dem Erzbischöflichen Ordinariat München und der Mitarbeitervertretung Erzbischöfliches Ordinariat München mit Unterzeichnung vom 9. Juni 2005 und 15. Juni 2018,

(D) Regelungen der Rahmendienstvereinbarung über die Einführung und den Einsatz von Informations- und Kommunikationssystemen im Zuständigkeitsbereich der Mitarbeitervertretung Erzbischöfliches Ordinariat München mit Unterzeichnung vom 2. Juni 2017 und 4. Juli 2017.

Bei Widersprüchen zwischen den Regelungen der unter Ziffer 1.5 (A) bis (D) genannten Regelungen und den Regelungen dieser IT-Nutzungsrichtlinie, gelten die Regelungen der unter Ziffer 1.5 (A) bis (D) genannten Regelungen vorrangig.

Soweit Dritte (z. B. externe dienstleistende Personen / Dienstleistungsunternehmen, selbstständige Rechtsträger, wie z. B. rechtlich selbstständige Stiftungen, u. a.) (ganz oder teilweise) Zugriff zu den IuK-Systemen erhalten, ist durch entsprechende vertragliche Vereinbarung mit diesen Dritten sicherzustellen, dass diese mindestens dasselbe Schutzniveau bei der Nutzung der IuK-Systeme zu beachten haben. Unbeschadet hiervon bleiben die Verpflichtungen nach § 21 KDG-DVO (externe Zugriffe, Auftragsverarbeitung).

2 Inhalt

2.1 Allgemeine Nutzungsbedingungen für die Nutzung der IuK-Systeme

(1) Die Nutzung der IuK-Systeme durch die Mitarbeiterinnen und Mitarbeiter hat ausschließlich zu dienstlichen Zwecken, d.h. insbesondere der Kommunikation zwischen den Mitarbeiterinnen und Mitarbeitern, mit anderen Einrichtungen der Erzdiözese, mit Geschäftspartnern und Abruf nützlicher dienstlicher Informationen zu erfolgen. Die Nutzung der IuK-Systeme zu privaten Zwecken ist unzulässig.

(2) Die Nutzung nicht dienstlich bereitgestellter oder freigegebener IuK-Systeme und Anwendungen (z. B. Cloud-Services und externe E-Mail-Konten) zum Zugriff, zur Verarbeitung oder Speicherung von dienstlichen Daten bedarf stets der vorherigen Zustimmung in Textform durch den Informationssicherheitsbeauftragten (R7.ISB) im Einzelfall oder durch eine gesonderte Richtlinie / Dienstvereinbarung.

(3) Unbeschadet der Regelung in Ziffer 2.1 (1) dieser IT-Nutzungsrichtlinie ist insbesondere folgende Nutzung der IuK-Systeme unzulässig:

- Es ist nicht gestattet, die IuK-Systeme zum Abrufen, Speichern oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen oder pornografischen Äußerungen oder Abbildungen zu verwenden. Eine Ausnahme besteht nur bei einem ausdrücklichen dienstlichen Auftrag zur Verarbeitung solcher Inhalte.
- Es ist nicht gestattet, die IuK-Systeme in Verletzung von Rechten Dritter (insbesondere Persönlichkeits-, Urheber-, Schutz- und Nutzungsrechte) zu nutzen. Hierzu zählen z. B. die Verwendung von Bildmaterial aus dem Internet ohne Nutzungsrechte, der illegale Download / Austausch von Software, Musik oder Videos (Filesharing) oder die Nutzung von Internetangeboten, welche nur zum Privatgebrauch bestimmt sind.
- Es ist nicht gestattet, vorsätzlich / wissentlich Schadprogramme (z. B. Viren, Würmer, Trojaner, Spyware, Keylogger) zu verwenden.

– Jede Nutzung der IuK-Systeme, die geeignet erscheint, den Interessen und dem Ansehen der katholischen Kirche und/oder der Erzdiözese in der Öffentlichkeit zu schaden, oder die gegen geltende Gesetze oder Verordnungen verstößt, ist unzulässig.

(4) Alle Mitarbeiterinnen und Mitarbeiter, welche die IuK-Systeme nutzen, haben sich wahrheitsgemäß, präzise und vollständig zu identifizieren. Insbesondere ist nicht gestattet, die eigene Identität bei der Nutzung von E-Mailsystemen der Erzdiözese zu verschleiern oder zu unterdrücken oder durch eine fremde Identität zu ersetzen bzw. eine solche zu fälschen.

(5) Für das Anlegen und den Umgang von Passwörtern haben die Mitarbeiterinnen und Mitarbeiter insbesondere die Verhaltensregelungen zum sicheren Umgang mit Passwörtern in der Erzdiözese München und Freising in der jeweils aktuellen Fassung zu beachten. Soweit einzelne Mitarbeiterinnen und Mitarbeiter von dem Geltungsbereich der Richtlinie Passworte im Erzbischöflichen Ordinariat München (technische und organisatorische Vorgaben) umfasst sind, haben diese Mitarbeiterinnen und Mitarbeiter die hierin enthaltenen Regelungen in der jeweils aktuellen Fassung zu beachten.

(6) Zur Gewährleistung der Datensicherheit und Verfügbarkeit müssen Dateien an Arbeitsplätzen und sonstigen IuK-Systemen der Erzdiözese auf vom Dienstgeber dafür bereitgestellten Netzlaufwerken im Betreuungsbereich der IT der Erzdiözese (z. B. derzeit Laufwerk H: oder Laufwerk I:) oder in einem durch den Dienstgeber bereitgestellten Dokumentenmanagementsystem gespeichert werden und dürfen nicht lediglich auf lokalen Laufwerken, insbesondere der lokalen Festplatte (C:) des Computers der Mitarbeiterin / des Mitarbeiters abgelegt werden. Hintergrund hierfür ist, dass Daten auf lokalen Laufwerken i.d.R. nicht Bestandteil der automatischen Datensicherung sind und in Fehlerfällen ggf. vollständig und unwiderruflich verloren gehen.

(7) Mitarbeiterinnen und Mitarbeiter haben insbesondere zur Gefahrenabwehr, aber auch zu Zwecken der Prävention alle ihnen bekannt gewordenen, möglicherweise sicherheitsrelevanten Ereignisse (z. B. Verlust, Diebstahl, Virenfund, Missbrauch von Kennungen, unerklärliches Systemverhalten, unerlaubte oder rechtswidrige Inhalte etc.) in Zusammenhang mit der Nutzung der IuK-Systeme unverzüglich zu melden.

Diese Meldung hat über die Hotline unter

089/ 21 37-17 00

zu erfolgen.

Weitergehende eigene Aufklärungsversuche durch Mitarbeiterinnen und Mitarbeiter sind erst nach vorheriger Zustimmung mit den für die Bearbeitung des Sicherheitsvorfalls Zuständigen (Helpdesk, IT-Abteilung, Informationssicherheitsbeauftragter, IT-Sicherheitsbeauftragter) zulässig. Insbesondere soll das Ausschalten (z. B. auch „Stecker ziehen“) von IuK-Systemen nur auf ausdrückliche Anweisung durch das Fachpersonal erfolgen.

(8) Das von Mitarbeiterinnen und Mitarbeitern zu beachtende Verfahren für den Umgang mit Datenschutzvorfällen (sicherheitsrelevante Ereignisse, bei welchen personenbezogene Daten betroffen sind/sein könnten) ist vom jeweiligen betrieblichen Datenschutzbeauftragten in einer Verfahrensanweisung („Vorgaben zur Meldung von Datenpannen und Maßnahmen zur Durchführung der Meldung“) geregelt.

2.2 Sorgfaltspflichten in Bezug auf den Umgang mit IuK-Systemen

(1) Mitarbeiterinnen und Mitarbeiter sind verpflichtet, die ihnen überlassene Hardware (wie z. B. Arbeitsplatzcomputer, Laptops, Token und andere transportable Geräte) mit der erforderlichen Sorgfalt vor Verlust, Diebstahl und Beschädigung zu schützen. Dies beinhaltet insbesondere, dass Laptops und andere transportable Geräte

- an öffentlich zugänglichen Orten stets beaufsichtigt werden müssen (auch kein Zurücklassen in Jacken, Mänteln, an der Garderobe etc.),
- wenn eine permanente Beaufsichtigung durch die Mitarbeiterin / den Mitarbeiter nicht möglich ist, durch geeignete Maßnahmen (Einschließen, Kabelschloss bei Laptops) vor einem Verlust, Diebstahl und Beschädigung geschützt werden müssen,
- über längere Zeit (z. B. über Nacht) nicht in Kraftfahrzeugen unbeaufsichtigt verbleiben dürfen bzw. auch bei kurzfristiger unbeaufsichtigter Ablage in Kraftfahrzeugen von außen nicht sichtbar sein dürfen (z. B. Einschließen in Kofferraum) und
- bei Flugreisen stets im Handgepäck mitgeführt werden müssen.

(2) Laptops und andere Mobilgeräte (auch mobile Endgeräte), die den Mitarbeiterinnen und Mitarbeitern durch die Erzdiözese bereitgestellt werden, dürfen durch dritte Personen nur unter Aufsicht der Mitarbeiterin / des Mitarbeiters genutzt werden. Die Verantwortung für den erforderlichen Schutz vor Verlust, Diebstahl und Beschädigung sowie zur Wahrung der Vertraulichkeit verbleibt immer bei der Mitarbeiterin / dem Mitarbeiter, dem das entsprechende Gerät vom Dienstgeber zur Verfügung gestellt wurde.

(3) Beim Einsatz von Laptops und anderen Mobilgeräten an öffentlich zugänglichen Orten (z. B. Flugzeug, Bahn) besteht stets die Gefahr des unerwünschten Mitlesens durch fremde Personen und damit die Gefahr, dass vertrauliche Informationen an die Öffentlichkeit gelangen. Daher dürfen interne, vertrauliche oder geheime Informationen und Dokumente an öffentlich zugänglichen Orten nicht geöffnet werden, sofern keine entsprechenden Schutzmaßnahmen durch die Mitarbeiterin / den Mitarbeiter getroffen werden (z. B. Sichtschutzfolie, geeignete Sitzplatzwahl).

(4) Beim Verlassen des Arbeitsplatzes müssen IuK-Systeme durch die Mitarbeiterin / den Mitarbeiter derart gesperrt werden, dass der Bildschirminhalt nicht mehr sichtbar ist und ein Entsperren nur durch Eingabe des Passworts / der PIN möglich ist. Ein Sperren ist zum Beispiel möglich, durch gleichzeitiges Drücken der „Windowstaste“ und des Buchstabens „L“.

(5) Nicht durch den Dienstgeber bereitgestellte Programme (z. B. aus dem Internet heruntergeladene Software) dürfen durch die Mitarbeiterin / den Mitarbeiter auf dienstlich bereitgestellten Geräten eigenmächtig weder installiert noch benutzt werden. Bei dienstlich bereitgestellten Mobilgeräten (Smartphones, Tablets) bezieht sich dies auch auf Apps, welche nicht durch den Dienstgeber bereitgestellt werden. Nicht vom Dienstgeber bereitgestellte Software darf auch dann nicht genutzt werden, wenn diese keine Installation benötigt, weil sie z. B. von einem Bootmedium (z. B. USB-Stick) aus gestartet werden kann.

(6) Einkauf, Installation, Änderungen, Umzug oder Reparatur der dienstlichen Hardware bzw. Software darf nur über den Dienstgeber beauftragt werden.

(7) Eingerichtete Sicherheitsmaßnahmen (Systemeinstellungen, Virenscanner, automatische Updates, Bildschirmsperren, Backups etc.) dürfen durch die Mitarbeiterin / den Mitarbeiter weder geändert noch deaktiviert werden.

(8) Mitarbeiterinnen und Mitarbeiter dürfen berechtigten Personen der Erzdiözese (z. B. Administratoren), nachdem diese sich authentifiziert haben (z. B. Dienstausweis), einen Zugang (physikalisch und elektronisch) zu Geräten im Eigentum der Erzdiözese nicht verweigern.

2.3 Netzwerkdienste

Um die Sicherheit von Netzwerken und zentralen Diensten nicht zu gefährden, dürfen Mitarbeiterinnen und Mitarbeiter folgende Aktivitäten nicht durchführen:

- Zugriffe auf eigene und fremde Ressourcen unter Umgehung von technisch/organisatorischen Schutzmaßnahmen oder unter Ausnutzung von Schwachstellen;
- Abhören des Netzwerkverkehrs oder der Einsatz von Werkzeugen zum Scannen nach Schwachstellen. Ausgenommen hiervon sind Mitarbeiterinnen und Mitarbeiter, die mit administrativen Aufgaben im Bereich der IT beauftragt sind, bzw. hierzu beauftragte dritte Unternehmen im Rahmen ihrer beauftragten Tätigkeit;
- Verbinden privater Geräte (z. B. Laptops) ohne vorherige Zustimmung mit Netzwerken der Erzdiözese (Soweit von der Erzdiözese Remotezugänge zur Verfügung gestellt werden, wie z. B. ORBIS, stellen diese keine Netzwerkverbindung im Sinne dieser Regelung dar.);
- Aufbau eigener WLANs mit Hilfe von nicht dienstlich bereitgestellten Geräten innerhalb der Dienststelle und die Verbindung dieser mit Netzwerken oder Geräten der Erzdiözese;
- Einrichtung eigener Kommunikationsverbindungen zwischen Systemen der Erzdiözese und externen Netzen (Internet) außerhalb der dienstlich bereitgestellten Zugangswege (z. B. über Mobilfunk-Sticks, WLAN);
- Nutzung von IuK-Systemen und Netzwerken, um externe oder fremde Dienste und Ressourcen anzugreifen oder auf Schwachstellen zu untersuchen.

2.4 Elektronische Kommunikation (E-Mail)

Ergänzend zu Ziffer 2.1 dieser IT-Nutzungsrichtlinie (Allgemeine Nutzungsbedingungen für die Nutzung der IuK-Systeme) sind die folgenden Anforderungen im Zusammenhang mit der Nutzung von E-Mail durch die Mitarbeiterinnen und Mitarbeiter zu beachten:

- Beim Versand von E-Mails tragen die Mitarbeiterinnen und Mitarbeiter die Verantwortung für einen vertraulichkeits- und datenschutzkonformen Umgang mit den Informationen. Dies gilt insbesondere bei E-Mail Adressen, welche nicht vom Dienstgeber bereitgestellt werden.
- Automatische Um- oder Weiterleitungen an E-Mail Adressen, welche nicht vom Dienstgeber bereitgestellt werden, dürfen nicht eingerichtet werden.

– Dateianhänge in auffälligen E-Mails, welche z. B.
  - von unbekannten Absendern stammen,
  - unaufgefordert / zusammenhanglos zugesendet werden, oder
  - in Sprache, Rechtschreibung oder Grammatik auffällig sind,

dürfen nicht ohne (z. B. telefonische) Vergewisserung beim Absender / bei der Absenderin geöffnet werden. Dasselbe gilt für Links in E-Mails zu externen Webseiten zur Abfrage von persönlichen Daten z. B. zur vermeintlichen Bestätigung von Bankdaten oder Benutzerkonten (Phishing).

Im Zweifel sind diese E-Mails an

ISMS@eomuc.de

zur Prüfung weiterzuleiten.

Zur Vermeidung von unerwünschter Werbung (Spam), hat die Weitergabe der dienstlichen E-Mail Adresse nach außen möglichst sparsam zu erfolgen. Eindeutig als Spam erkennbare Nachrichten sind ungeöffnet an das Postfach spam@eomuc.de weiterzuleiten und danach zu löschen, da teilweise schon das Öffnen einer Nachricht dem Absender anzeigt, dass es sich um eine gültige und aktive Empfängeradresse handelt. Bei massivem Auftreten von Spam ist die Hotline unter 089/ 21 37-17 00 zu kontaktieren.

Das Absenden von Spam über die IuK-Systeme ist untersagt.

3 Inkrafttreten dieser Richtlinie

Diese IT-Nutzungsrichtlinie für die Erzdiözese München und Freising KdöR tritt am 1. Juni 2021 in Kraft und gilt auf unbestimmte Zeit. Sie wird im Amtsblatt für das Erzbistum München und Freising veröffentlicht.

München, den 25. Mai 2021

Christoph Klingan
Generalvikar

Dr. Stephanie Herrmann
Amtschefin

80. Neues Pfarrsiegel der Pfarrei Litzldorf-St. Michael

Die Pfarrei Litzldorf-St. Michael hat ein neues Pfarrsiegel fertigen lassen.

Gemäß § 10 Abs. 4 der Siegelordnung für das Erzbistum München und Freising (Amtsblatt 2009, Nr. 15, S. 387–390) wird der Abdruck des neuen Siegels nachstehend veröffentlicht. Mit der Veröffentlichung im Amtsblatt ist das neue Siegel zur Verwendung freigegeben.



Abdruck des neuen Siegels
der Pfarrei Litzldorf-St. Michael

Das alte Siegel, dessen Abdruck nachstehend veröffentlicht wird, wird für ungültig erklärt und ist außer Gebrauch zu nehmen. Das alte Siegel ist im Pfarrarchiv aufzubewahren oder dem Diözesanarchiv zu übergeben.



Abdruck des für ungültig erklärten alten Siegels
der Pfarrei Litzldorf-St. Michael