

Richtlinie zur Nutzung der informations- und kommunikationstechnischen Anlagen (IKA) des Bistums Dresden-Meißen

Die Sicherheit und der Schutz der personenbezogenen Daten von Mitarbeitern¹, Geschäftspartnern und Dritten sind auch vom fehlerfreien Funktionieren der informations- und kommunikationstechnischen Anlagen abhängig. Dazu gehören die Infrastrukturbestandteile der elektronischen Datenverarbeitung (IT), feste und mobile Endgeräte sowie Telefonanlagen. Durch Schadsoftware, Spionage und Sabotage sind diese Anlagen besonders gefährdet. Unsachgemäße Nutzung, bewusster und unbewusster Missbrauch erhöhen nicht nur das Gefährdungspotential. Sie verursachen erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung sowie die ausfallsichere Auslegung der IKA-Komponenten.

Um die Sicherheit und den Schutz der IKA sowie der gespeicherten Daten zu gewährleisten und die Kosten in akzeptablen Grenzen zu halten, ist es notwendig, dass die Nutzer mit der Technik verantwortungs- und kostenbewusst umgehen. Die Bestimmungen des KDG und der KDG-DVO sind einzuhalten. Jeder Mitarbeiter, der gegen die vorstehenden Regeln verstößt, muss mit arbeitsrechtlichen Sanktionen bis hin zur – auch fristlosen – Kündigung rechnen. Darüber hinaus haftet jeder Nutzer gemäß den allgemeinen Grundsätzen auf Schadenersatz.

Die nachfolgend genannten Vorschriften sind deshalb von allen Nutzern der IKA des Bistums Dresden-Meißen sowohl in den Dienststellen als auch bei Tätigkeiten außerhalb (z.B. bei Reisen oder mobilem Arbeiten) einzuhalten.

1. In den IKA des Bistums, insbesondere auf allen Servern, Computern, Laptops sowie den dienstlichen Bereichen anderer mobiler Endgeräte dürfen nur Anwendungen (Software) installiert und genutzt werden, die vom Generalvikar oder vom IT-Leiter (LIT)² des Bistums frei gegeben sowie korrekt lizenziert wurden. Ausnahmen von dieser Regelung (z.B. der Testbetrieb neuer Software oder aktualisierter Softwareversionen) bedürfen der Genehmigung des LIT.
2. Die Installation von Software darf ausschließlich durch Personen erfolgen, die vom LIT damit beauftragt wurden. Insbesondere gelten folgende Regelungen:
 - Betriebssysteme, Anwendungsprogramme, Updates, Patches und Hotfixes dürfen nur von Beauftragten des LIT lizenziert und installiert werden.
 - Nutzer dürfen ohne Befugnis keine Software aus dem Internet herunterladen oder auf anderem Weg auf Computern installieren. Dazu gehören auch Bildschirmschoner, Demoprogramme, Computerspiele oder Hilfsprogramme.
 - Ohne besondere Genehmigung dürfen keine aus dem Internet heruntergeladenen oder per E-Mail (Anhänge) oder Datenträgern übermittelte Anwendungen gestartet werden.
 - Alle Datenbestände, von außerhalb (z.B. auf externen Datenträgern wie externen Festplatten, Speicherkarten, Memory-Sticks etc.) müssen vor Verwendung durch die jeweils aktuelle Anti-schadsoftware überprüft werden.
3. Nicht ausdrücklich befugte Nutzer dürfen weder von zugekaufter noch von selbst erstellter Software Kopien erstellen. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.

¹ Zur Wahrung bestmöglicher Verständlichkeit wird in dieser Richtlinie für Personen nur die männliche Form verwendet. Sie gilt jedoch auch für alle anderen Personen.

² Sofern eine Bistumseinrichtung ihre IT in eigener Verantwortung betreibt, werden die Rechte und Pflichten des LIT durch den Leiter / die Leiterin der Einrichtung ausgeübt.

4. Soweit Dritte (z.B. externe Dienstleister) ganz oder teilweise Zugriff zu den IKA erhalten, ist durch entsprechende vertragliche Vereinbarung sicherzustellen, dass diese mindestens dasselbe Schutzniveau für die Daten gewährleisten. Die Verpflichtungen nach § 21 KDG-DVO bleiben unberührt.
5. Die private Nutzung der IKA durch Dritte ist in jedem Fall unzulässig.
6. Alle Nutzer der IKA haben sich wahrheitsgemäß zu authentifizieren. Insbesondere ist nicht gestattet, die eigene Identität bei der Nutzung von dienstlichen E-Mailsystemen zu verschleiern oder zu unterdrücken oder durch eine fremde Identität zu ersetzen bzw. eine solche zu fälschen. Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder als Papier-Notiz noch als Datei auf Computern oder Datenträgern. Vom LIT können nach vorheriger Prüfung s.g. Passwortsafes zugelassen werden. Administrative Passwörter und dienstliche Zugangscodes müssen in einem versiegelten Umschlag im Tresor des Generalvikars oder des Justitiars oder des Leiters der Einrichtung hinterlegt werden. Passwörter dürfen unter keinen Umständen an andere Personen weitergegeben werden.
7. Nutzer sind verpflichtet, die ihnen überlassene Hardware (wie z.B. Arbeitsplatzcomputer, Laptops, Smartphones) mit der erforderlichen Sorgfalt vor Verlust, Diebstahl und Beschädigung zu schützen. Dies beinhaltet insbesondere, dass Laptops und andere mobile Geräte an öffentlich zugänglichen Orten stets zu beaufsichtigen sind. Sofern permanente Beaufsichtigung (z.B. in Garderoben) nicht möglich ist, ist das Gerät durch geeignete Maßnahmen (mitnehmen, einschließen) vor Verlust oder Beschädigung zu schützen. Geräte dürfen über längere Zeit (z.B. über Nacht) nicht in Kraftfahrzeugen unbeaufsichtigt verbleiben und auch bei kurzfristiger unbeaufsichtigter Ablage von außen nicht sichtbar sein. Bei Flugreisen sind sie stets im Handgepäck mitzuführen.
8. Beim Einsatz von Laptops und anderen Mobilgeräten an öffentlich zugänglichen Orten (z.B. Verkehrsmitteln) besteht stets die Gefahr des unerwünschten Mitlesens durch fremde Personen und damit das Risiko, dass vertrauliche Informationen an die Öffentlichkeit gelangen. Daher dürfen interne Informationen und Dokumente an öffentlich zugänglichen Orten nur geöffnet werden, sofern entsprechenden Schutzmaßnahmen (z.B. Sichtschutzfolie, geeignete Sitzplatzwahl) getroffen werden.
9. Beim Verlassen des Arbeitsplatzes müssen IKA durch den Nutzer so gesperrt werden (Windowstaste + L), dass der Bildschirminhalt nicht mehr sichtbar ist und ein Entsperren nur durch Eingabe des Passworts/der PIN möglich ist.
10. Nutzer dürfen berechtigten Personen (z.B. Administratoren)³ den physischen und elektronischen Zugang zu Geräten im Eigentum des Bistums nicht verweigern.
11. Jeder Nutzer hat alle ihm im Rahmen seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich zu behandeln bzw. geheim zu halten, soweit dies geboten ist. Er darf derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben, es sei denn, gesetzliche Pflichten erfordern dies.
12. Nutzer dürfen nicht versuchen, auf Bereiche von Netzwerken vorzudringen, die nicht für den Nutzer und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte oder der LIT ohne Verzug zu informieren.
13. Nutzer dürfen nicht nach Schwachstellen in den IKA suchen.

³ Sofern der Administrator dem Nutzer nicht persönlich bekannt ist, hat er sich dadurch zu legitimieren, dass er sich am Gerät unter seinem Admin-Zugang erfolgreich anmeldet.

14. Private Geräte (z.B. Laptops) dürfen ohne vorherige Zustimmung des LIT nicht mit den Netzwerken des Bistums verbunden werden. Die Nutzung von für private Zwecke eingerichteten WLAN ist jedoch zulässig. Die bloße Anzeige von dienstlichen Daten auf Privatgeräten ist zulässig, wenn die Datenvertraulichkeit gewahrt bleibt.
15. Der Aufbau eigener WLANs innerhalb der Dienststellen mit Hilfe von privaten Geräten ist nicht erlaubt.
16. IKA des Bistums dürfen nicht verwendet werden, um fremde Dienste und Ressourcen anzugreifen oder auf Schwachstellen zu untersuchen.
17. Eingerichtete Sicherheitsmaßnahmen (Systemeinstellungen, Virens Scanner, automatische Updates, Bildschirmsperren, Backups, etc.) dürfen durch den Nutzer weder geändert noch deaktiviert werden.
18. Bei Verdacht auf Schadsoftware, Datenspionage oder anderer Umstände, die die Sicherheit der IKA betreffen, ist unverzüglich der Vorgesetzte oder der LIT zu informieren.
19. Störungen und Defekte der IKA und auftretende Fehler in der Software sind unverzüglich den dafür verantwortlichen Personen zu berichten.
20. Mitarbeiter, die mit der Datensicherung beauftragt sind, haben diese Aufgaben mit besonderer Sorgfalt durchzuführen und müssen den Vorgesetzten unverzüglich informieren, wenn Probleme auftreten.
21. Zur Gewährleistung von IT-Sicherheit und -Kompatibilität erfolgen Anschaffungen, Änderungen, Umzüge oder Reparaturen von IT-Hardware aller Art, mit Ausnahme einfacher Speichermedien (USB-Sticks, Speicherkarten), ausschließlich durch das Referat Zentrale Dienste des Bischöflichen Ordinariats. Vor Anschaffung von Geräten mit IT-Schnittstellen (Kameras, ...) ist das Votum der Zentralen Dienste einzuholen.⁴
22. Jeder Nutzer ist angehalten, die technischen Anlagen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchsmaterialien wie Druckerpapier, Druckfolien, Druckerpatronen usw.
23. Dienstliche Daten dürfen auf Geräten in Privateigentum nur dann verarbeitet werden⁵, wenn sie mit vom LIT zugelassenen Maßnahmen geschützt wurden. Die Nutzung von privat eingerichteten Cloud-Services oder E-Mail-Konten ist unzulässig. Ausnahmen für Daten der Datenschutzklasse I sind zulässig, wenn die Maßgaben der KDG-DVO (§20 Abs. 2) eingehalten werden. Die ggf. notwendige Entscheidung trifft der Generalvikar.
24. Dienstliche Daten müssen - soweit dies technisch möglich ist (mobile Endgeräte) - generell so gespeichert werden, dass bei Ausfall eines Nutzers dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann. Für die Speicherung von dienstlichen Daten ist das persönliche Verzeichnis, auf das nur der jeweilige Nutzer über sein Passwort zugreifen kann, nicht geeignet. Dienstliche Daten sind generell in Gruppenverzeichnissen abzulegen. Damit bei Ausfall eines Nutzers diese Daten von anderen Nutzern gefunden werden, muss die Ordnerstruktur im Gruppenverzeichnis auf den Servern ständig beachtet werden. Namen für Ordner oder Dokumente sollen eindeutig gewählt werden.
25. Jeder Nutzer soll nicht mehr benötigte Dateien und E-Mails regelmäßig löschen, um die Datenbestände und deren Strukturen überschaubar und die Kosten der Datenhaltung und Datensicherung

⁴ Die unter Ziff. 21 genannte Regelung gilt nicht für Bistumseinrichtungen, die ihre IT in eigener Verantwortung (siehe IT-Strategie des Bistums) betreiben.

⁵ Verarbeitung von Daten (Änderung, Speicherung) ist von der bloßen Anzeige von Daten auf dem Endgerät zu unterscheiden.

in vertretbaren Grenzen zu halten. Die Löschung darf nicht erfolgen, sofern die gesetzlichen Vorschriften, die Kirchliche Archivordnung (KA 22/2014) oder anderweitige innerkirchliche Regularien die Aufbewahrung vorschreiben.

26. Jeder Nutzer des dienstlichen Mailsystems hat dafür zu sorgen, dass bei absehbarer Abwesenheit von mehr als zwei Tagen (ohne Zugriffsmöglichkeit auf das Postfach) eine Abwesenheitsnotiz eingerichtet wird. In dieser sollen die Kontaktinformationen des Vertreters benannt werden. Automatisierte Weiterleitung von E-Mails ist nicht zulässig.
27. Sofern aus dringenden dienstlichen Gründen ein Zugriff auf die Inhalte des elektronischen Postfaches erforderlich ist und der Inhaber des Postfaches nicht rechtzeitig erreicht werden kann, dürfen Administratoren auf Anweisung des Generalvikars Zugriff auf die Inhalte des Postfachs nehmen und Informationen an die Zuständigen weiter geben. Erfolgreiche Kontaktversuche, Gründe und der Umfang des Zugriffs sind zu dokumentieren. Der Nutzer ist hierüber baldmöglichst zu informieren.
28. Ist absehbar, dass ein Nutzer die IKA des Bistums für einen Zeitraum von mehr als 6 Monaten nicht mehr anwendet, hat er private Daten sowie nicht mehr benötigte dienstliche Datenbestände und E-Mails zu löschen. Er hat die verbleibenden Datenbestände an den unmittelbaren Vorgesetzten (ehrenamtliche IT-Nutzer: an die fachlich zuständige Stelle) oder die Registratur zu übergeben. Vorgesetzte stellen die ordnungsgemäße Übernahme der Datenbestände sicher. Wenn eine geordnete Übergabe unter Beteiligung des Nutzers nicht möglich, Datenzugriff zu dienstlichen Zwecken aber dringend erforderlich ist, dürfen Administratoren auf Anweisung des Generalvikars Zugriff auf die vorhandenen Daten nehmen. Offensichtlich private Inhalte sind von dieser Regelung ausgenommen.
29. Die IKA dürfen grundsätzlich nicht für private Zwecke gebraucht werden. Ausnahmen gelten für die private Nutzung hierfür vorgesehener, drahtlose Netzwerke (vgl. Ziff. 14) sowie von Internetdiensten (siehe Ziff. 31). Die Restriktion gilt ferner nicht für dienstliche mobile Endgeräte, sofern auf diesen private und dienstliche Daten getrennt verwaltet und letztere angemessen geschützt werden. Auf den dienstlichen Arbeitsplatz-Computern dürfen prinzipiell keine privaten Daten gespeichert werden.
30. Die Nutzung von Internetdiensten werden gemäß Anlage 1 protokolliert. Sollten Nutzer hiermit nicht einverstanden sein, ist die Nutzung nicht zulässig. Aus der Nutzung der Internetdienste dürfen keine zusätzlichen Kosten ohne dezidierte Zustimmung des Budgetverantwortlichen und des LIT entstehen. Datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen sowie sonstige Rechtsvorschriften sind einzuhalten. Inhalte mit beleidigenden, verleumderischen, verfassungsfeindlichen, gewaltverherrlichenden, rassistischen, sexistischen oder pornografischen Äußerungen und Abbildungen dürfen nicht abgerufen werden. Die Interessen des Bistums und anderer Körperschaften der katholischen Kirche sind in jedem Fall zu wahren.
31. Internetdienste dürfen am Arbeitsplatz grundsätzlich nur dienstlich genutzt werden. Die private Nutzung in geringfügigem Umfang ist zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit der IT-Systeme für dienstliche Zwecke nicht beeinträchtigt werden. Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch ist unzulässig. Die Erlaubnis der privaten Nutzung des zur Verfügung gestellten Internetzugangs ist auf das Abrufen von Inhalten beschränkt. Private Daten dürfen nur in einem als „privat“ gekennzeichneten Ordner in sehr geringem Umfang gespeichert werden. Nicht mehr benötigte Inhalte sind zu löschen. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden.
32. Die private Nutzung der dienstlichen E-Mail-Adresse ist in jedem Falle untersagt. Sollten dennoch private E-Mails eingehen, sind diese umgehend zu löschen. Zudem sind die Absender der E-Mails vom Nutzer darauf hinzuweisen, dass dieser die dienstliche E-Mail-Adresse nur zu dienstlichen Zwecken

nutzen darf. Den IT-Administratoren ist im konkreten Verdachtsfall missbräuchlicher Nutzung und nur auf Anweisung des Generalvikars sowie vorheriger Information der MAV und des betrieblichen Datenschutzbeauftragten die Einsicht und die Nutzung von Protokolldaten für die Prüfung der Systemsicherheit und -integrität sowie der Einhaltung zur Nutzungsbeschränkungen gestattet.

33. Zur Vermeidung des Zugriffs auf unzulässige oder die IT-Sicherheit gefährdende Inhalte wird der Zugriff auf bestimmte Internetseiten und Internetdienste zentral gesperrt. Diese Restriktion betrifft insbesondere auch Anhänge von E-Mails. Soweit trotz Filterung E-Mails eingehen, deren Absender oder Inhalt zweifelhaft erscheinen, sind diese ungeöffnet zu löschen.

Diese Richtlinie tritt mit Ihrer Veröffentlichung in Kraft. Gleichzeitig tritt die Dienstanweisung zur „Datensicherheit sowie zur verantwortungsvollen- und kostenbewussten Nutzung der informationstechnischen Anlagen der Einrichtungen des Bistums Dresden-Meißen“ vom 2. August 2021 außer Kraft.

Dresden, den 21.03.2023

gez. Andreas Kutschke, Generalvikar

Protokollierung

- (1) Das E-Mail-System führt Protokolldateien (Sender, Empfänger, Betreff, Zeitangabe, Größe) über ein- und ausgehende E-Mails. Inhalte der E-Mails werden nicht protokolliert. Jedoch werden die E-Mails in Gänze auf zentralen Systemen (Exchange-Server) gespeichert, solange das jeweilige Postfach existiert und der Nutzer die Mails nicht löscht. Aus den turnusmäßigen Back-Ups sind auch vormals gelöschte Postfächer und E-Mails wiederherstellbar.
- (2) Im Zusammenhang mit der Nutzung des Internets werden
 - die IP-Adresse des abrufenden Arbeitsplatz-PCs,
 - die kontaktierten Webserver und ggf. die aufgerufenen Internetseiten,
 - das Datum und die Uhrzeit des Abrufs,
 - die Datenvolumina,
 - alle abgewiesenen Verbindungsversuche aus dem Internet,
 - alle abgewiesenen Verbindungsversuche der Nutzer,
 - alle Verbindungen auf Sicherheitssysteme und
 - alle Sitzungen der zentralen Fernwartungslösungaufgezeichnet bzw. protokolliert. Bei Datenverbindungen über Proxy-Systeme; werden neben den URLs auch die IP-Adressen der eigentlichen Proxys aufgezeichnet.
- (3) Alle Protokolle der zentralen Komponenten werden für den laufenden und maximal die letzten fünf Monate vorgehalten und danach unwiederbringlich gelöscht.
- (4) Jede Auswertung von Protokolldaten muss die Regelungen des Datenschutzes berücksichtigen, insbesondere den Grundsatz der Verhältnismäßigkeit.
- (5) Die für den Datenschutz und die Sicherheit der technischen Systeme zuständigen Administratoren sind berechtigt, die erhobenen Protokolldaten unter Bildung von Pseudonymen zu statistischen Zwecken auszuwerten. Sofern bei der statistischen Auswertung der begründete Verdacht entsteht, dass eine unzulässige Nutzung stattfand, erfolgt nach Rücksprache mit dem Generalvikar eine personenbezogene Auswertung der betroffenen Protokolldaten. Der betriebliche Datenschutzbeauftragte und die Mitarbeitervertretung werden vor Durchführung der Auswertung informiert. Der Umfang der personenbezogenen Auswertung sowie die Gründe sind schriftlich zu dokumentieren. Die von der Auswertung betroffenen Nutzer sind über die Auswertung zu informieren. Bei dem Vorliegen des Verdachts von Straftaten können die Strafverfolgungsbehörden eingeschaltet und Beweise gesichert werden.
- (6) Gesetzlich geregelte Datenverarbeitungen bzw. gesetzlich geregelte Eingriffe in das Fernmeldegeheimnis bleiben von den vorstehenden Regelungen unberührt. Dies gilt insbesondere für Maßnahmen der Störungsprävention und dem Schutz der technischen Systeme.
- (7) Die Nutzung der Protokolldaten zu allgemeinen Leistungs- oder Verhaltenskontrollen ist nicht zulässig. Davon unberührt bleibt die Auswertung von Daten gemäß den Regelungen dieser Erklärung oder anderer Rechtsvorschriften.