

Dienstanweisung zur Nutzung der Informationstechnologie im Erzbistum Berlin

Für dieses Dokument ist die IT-Abteilung des Erzbischöflichen Ordinariats verantwortlich. Das Dokument, insbesondere dessen Anlagen unterliegt einer stetigen Revision zum Erhalt der Aktualität. Zur besseren Lesbarkeit wird das generische Maskulinum verwendet.

1.	Allgemeine Richtlinie zum Umgang mit der Informationstechnologie	3
2.	Benutzerkonten	4
3.	Rechte- und Rollenkonzept	5
4.	Datenmanagement.....	6
4.1	Personenbezogene Daten	6
4.2	Datenklassifizierung	6
4.3	Per Backup abgesicherte Speicherorte	7
4.4	Transkription	7
5.	Umgang mit IT-Komponenten	8
5.1	Software und Fachanwendungen	8
5.2	E-Mails und E-Mail-Konten	9
5.2.1	Vorlage Signatur.....	10
5.2.2	Vorlage Abwesenheitsnotiz	10
5.2.3	Rechtsverbindlicher Empfang von E-Mails	11
5.2.4	Versand personenbezogener und vertraulicher Daten	11
5.2.5	Erläuterungen zu E-Mail-Komponenten und -Funktionen.....	11
5.3	PC-Endgeräte (Desktop / Laptop)	13
5.4	Smartphones aus dem Mobile Device Management.....	13
5.5	Künstliche Intelligenz (KI).....	13
5.6	Öffentliche Netzwerke	15
6	Support	16
7	Schulungen	17
8	Notfallmanagement.....	18
9	Anhänge.....	19
	Versionierung	20
	Zusammenfassung.....	22

1. Allgemeine Richtlinie zum Umgang mit der Informationstechnologie

Diese Richtlinie gilt für die vom Teilbereich R.IV.1 Digitalisierung sowie deren IT-Dienstleister verantworteten Informationstechnologieinfrastruktur sowie der darin genutzten Fachanwendungen.

Dies betrifft in der aktuellen Version

- das Bischofsbüro,
- alle Mitarbeiter des Erzbischöflichen Ordinariats in der Niederwallstraße,
der Bruno-Möhring-Straße,
der Ahornallee,
den Pfarreien des Erzbistums Berlin,
der Kategorialen Seelsorge,
dem Katholischen Büro,
dem Offizialat.

Wird die vom Teilbereich R.IV.1 Informationstechnologie und deren Dienstleister verantwortete IT-Infrastruktur sowie die darin genutzten Fachanwendungen von Mitarbeitenden der Pfarreien genutzt, so sind diese auf die Inhalte der jeweils gültigen Dienstanweisung zu verpflichten.

Die Einhaltung der Dienstanweisung ist entscheidend für die Sicherheit und den Schutz der IT-Infrastruktur des Erzbistums Berlin.

Grundsätzlich erfordern alle Neuerungen bzw. Änderungen an Komponenten dieser IT-Infrastruktur einer expliziten Zustimmung des Teilbereichsleiters R.IV.1 und des Bereichsleiters R.IV Bistumsinterne Organisation.

Beim Einsatz von Informationstechnologie im Erzbistum Berlin ist es untersagt, Inhalte abzurufen, zu verbreiten oder zu speichern, die gegen Persönlichkeits-, Datenschutz-, Lizenz-, Urheber- oder Strafrecht verstoßen.

Es ist ebenso verboten, beleidigende, verleumderische, verfassungsfeindliche, rassistische, sexistische, gewaltverherrlichende oder pornografische Inhalte abzurufen, zu verbreiten oder zu speichern.

Es ist nicht gestattet, andere dazu zu ermutigen oder zu unterstützen, gegen diese Vorgaben zu verstoßen.

Ein Verstoß gegen diese Dienstanweisung kann zur Sperre oder gesamten Deaktivierung von Endgeräten sowie Benutzerkonten führen.

2. Benutzerkonten

Nutzer erhalten personalisierte Benutzerkonten mit den Domains erzbistumberlin.de oder ebo-cloud.de. Darüber hinaus gibt es Funktionskonten, die sich mehrere Nutzer teilen (z. Bsp. it.helpdesk@erzbistumberlin.de).

Alle Benutzerkonten sind mit starken Passwörtern und Multi-Faktor-Authentifizierung geschützt.

Das Passwort eines Benutzerkontos darf nicht weitergegeben werden.

Grundsätzlich sollen sich Passwörter gemerkt und nicht dokumentiert werden (z. Bsp. keine Klebezettel am Monitor, nicht innerhalb einer Datei auf dem Endgerät oder einer Mail im E-Mail-Postfach etc.).

Das Speichern in Webbrowsern (z. Bsp. Firefox, Edge, Chrome etc.) ist nicht gestattet.

Die Nutzung der Benutzerkonten ist nur in der vom Teilbereich R.IV.1 Informationstechnologie verantworteten Informationstechnologieinfrastruktur sowie der darin genutzten Fachanwendungen gestattet.

Die private Nutzung der Benutzerkonten ist untersagt. Die Nutzung der Benutzerkonten auf privaten Geräten über den von Microsoft zur Verfügung gestellten Login der Webseite <https://www.office.com> ist untersagt.

E-Mailadressen @erzbistumberlin.de und @ebo-cloud.de dürfen nicht an private E-Mailadressen weitergeleitet werden.

Für die Nutzung von privaten Endgeräten im Zuge der Arbeit von zu Hause wird eine Virtual-Private-Network (VPN) mit Remote-Desktop-Zugriff (RDP) zur Verfügung gestellt. Innerhalb dieser Lösung ist die Nutzung von office.com für den Zugriff auf SharePoint-Daten möglich (Speicherorte MS Teams und OneDrive).

Die Teilnahme an digitalen Konferenzen über Konferenzsoftware (z. Bsp. Zoom, Webex, MS Teams etc.) über private Geräte bei der Arbeit von zu Hause bzw. im Home-Office ist möglich.

Die Kontenverwaltung, die ggfs. in Fachanwendungen zum Einsatz kommt, muss sich an die Sicherheitsrichtlinien dieser Dienstanweisung orientieren, um einen hohen Schutzgrad zu erreichen.

3. Rechte- und Rollenkonzept

Grundsätzlich gilt für alle Rechte- und Rollenkonzepte folgendes Vergabeprinzip: Es werden nur die am Arbeitsauftrag Beteiligten sowie zu informierenden Personen mit den jeweils dafür notwendigen Rechten ausgestattet. Derjenige Mitarbeitende, welcher den Arbeitsprozess führt, zeichnet sich dafür verantwortlich.

Eine Dateneinsicht soll nur für autorisierte Personen erfolgen. Insofern ein Zugriff auf nicht benötigte, vertrauliche oder interne bzw. personenbezogene Daten besteht, ist diese dem Vorgesetzten und dem Datenschutz zu melden und der Koordinator für den Datenschutz unverzüglich zu informieren.

Für die Aktualität des Rechte- und Rollen-Systems ist ein funktionierender Prozess zum zeitnahen Melden von Eintritten, Austritten und Wechseln im Personal zu pflegen.

Jedes Rechte- und Rollensystem muss einer regelmäßigen Revision unterliegen, um auf systembedingte und inhaltliche Änderungen reagieren zu können. Der bzw. die Verantwortliche(n) des Systems sind für die Revision verantwortlich.

Insofern vorher vorhandene Rechte zur Erledigung eines Arbeitsauftrags nicht mehr benötigt werden, weil dieser sich z. Bsp. verändert hat, sind diese zu entfernen.

Rechte- und Rollenkonzepte aus Fachanwendungen unterliegen der Verantwortung des jeweiligen Fachbereichs.

4. Datenmanagement

Zu jeder Zeit hat der Umgang mit Daten konform zum Gesetz über den Kirchlichen Datenschutz (KDG) zu erfolgen.

Dienstliche Informationen bzw. dienstliche Daten jeder Art sind nur auf Dienstgeräten bzw. in Dienstumgebungen zu speichern.

Die Verwendung von privaten Datenträgern (externe Festplatten / USB-Sticks) zum Speichern oder Transferieren ist ausnahmslos untersagt.

Informationen bzw. Daten, die im Zuge von Administrationsoberflächen eingesehen und / oder genutzt werden können, dürfen nur zu Supportzwecken nicht für eine Leistungs- und Verhaltenskontrolle verwendet werden.

4.1 Personenbezogene Daten

Gemäß § 4 Nr. 1 des Gesetzes über den kirchlichen Datenschutz (KDG) sind personenbezogene Daten definiert als: „Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.“

Eine identifizierbare natürliche Person ist jemand, der direkt oder indirekt identifiziert werden kann. Dafür können u. a. die folgenden Merkmale Verwendung finden: Name, Kennnummer, Standortdaten, IP-Adresse, Adresse, Telefonnummer, E-Mail-Adresse, Kontodaten, Kreditkartennummer uvm.

Auch indirekte Informationen können personenbezogen sein, wenn sie mit anderen Daten kombiniert eine Identifizierung ermöglichen.

Juristische Personen (z. B. GmbHs) sind nicht durch das KDG geschützt.

4.2 Datenklassifizierung

Wie in 4.1 beschrieben wird unterschieden in personenbezogene Daten, die per KDG geschützt werden, und in nicht personenbezogene Daten.

Darüber hinaus wird in folgende Klassifizierungen unterschieden:

Öffentlich:

Diese Informationen stehen der Öffentlichkeit zur Verfügung. Hierzu gehören z. Bsp. Informationen auf den Webseiten (z.B. <https://www.erzbistumberlin.de>) - außerhalb des passwortgeschützten Bereichs.

Intern:

Interne Informationen sind nur für Mitarbeiter im Erzbistum Berlin zugänglich und sind somit gegen unbefugten Zugriff zu schützen.

Vertraulich:

Vertrauliche Informationen sind nur für einen Teil der Mitarbeiter im Erzbistum Berlin zugänglich und sind daher weitergehend mit einem Rechte-Rollen-Konzept bzw. -System zu schützen.

4.3 Per Backup abgesicherte Speicherorte

Sämtliche Daten sollen an Orten gespeichert werden, die mit Backups abgesichert werden. Dazu gehören die folgenden Speicherorte:

- Netzlaufwerke
- Regisafe
- OneDrive
- MS Teams

Das dient der Wiederherstellmöglichkeit der Daten im Verlustfall des Endgerätes.

4.4 Transkription

Mit MS Teams können Transkripte von digitalen Sitzungen automatisiert erstellt werden. Eine Transkription bedarf einer expliziten Zustimmung durch alle Teilnehmer, für die das Transkript erstellt wird.

Eine solche Zustimmung wird beim Einschalten der Transkription während einer digitalen Sitzung von allen digital anwesenden Teilnehmern eingeholt.

Dabei wird betont, dass jede Zustimmung freiwillig erfolgen muss und unter keinen Umständen erzwungen werden darf, und jederzeit widerrufen werden kann, was das unverzügliche Beenden der Transkription sowie das Löschen des bis dahin erstellten Transkripts erzwingen würde.

Eine Transkription darf nur für Sitzungen stattfinden, die eines der folgenden Kriterien erfüllen:

- Dokumentation wichtiger Entscheidungen oder Vereinbarungen
- Erfüllung gesetzlicher Pflichten
- Nachvollziehbarkeit komplexer Projekte oder die Bereitstellung von Informationen für abwesende Mitarbeiter

Das Transkript wird im Chatverlauf der Sitzung veröffentlicht. 48 Stunden nach dem Erstellen sind Transkripte zu löschen. Die Löschung ist im Programm MS Teams vorzunehmen.

5. Umgang mit IT-Komponenten

5.1 Software und Fachanwendungen

Die private Nutzung von Software und Fachanwendungen ist untersagt.

Bevor eine Software eingesetzt werden kann, muss

- die Zustimmung der betroffenen Mitarbeitervertretungen,
- eine Freigabe der zuständigen Bereichsleitung bei Fachanwendungen sowie
- die Freigaben des Teilbereichsleiters Digitalisierung und des Bereichsleiters Bistumsinterne Organisation vorliegen.

Insofern die Software personenbezogene Daten verarbeiten soll, ist über ZS. 8 eine Freigabe des Datenschutzbeauftragten zu erwirken.

Sollten Auftragsdaten verarbeitet werden, ist unter Beteiligung von ZS. 8 eine Vereinbarung zur Auftragsdatenverarbeitung mit dem Softwarehersteller abzuschließen.

Die Anwendungen MS Planner, MS ToDo, MS Project, Copilot dürfen nicht zur Leistungs- und Verhaltenskontrolle verwendet werden, solange keine gültige Dienstvereinbarung verabschiedet wurde, mit der die Leistungs- und Verhaltenskontrolle ermöglicht wird.

Die Anwendung MS Forms, die zum Erstellen von Umfragen verwendet werden kann, soll, soweit es der Anwendungszweck zulässt, für die anonymisierte Datenerhebung genutzt werden.

Die Nutzung von MS Forms und MS Project ist besonders in Bezug auf eingebaute Freitextfelder zu überprüfen und die Nutzer darauf hinzuweisen, dass in Freitextfelder nach Möglichkeit keine personenbezogenen Daten eingetragen werden sollen.

Es dürfen grundsätzlich keine besonders sensiblen Daten in Freitextfelder gespeichert werden.

Bei der Nutzung von PowerBI, eine Anwendung zum Erstellen automatisierter Statistiken und Berichte, muss eine menschlichen Plausibilitätsprüfung (analog zur Verwendung von KI-Ergebnissen) erfolgen. Die Statistiken und Berichte dürfen nicht als alleinige Entscheidungsgrundlage dienen und sind durch Personen zu prüfen.

Finanzdaten müssen dahingehend anonymisiert werden, dass keine Rückschlüsse auf sensible Informationen von Personen (z. Bsp. Gehalt einer HHST mit einem Angestellten) ermöglicht werden. Veröffentlichte Berichte sind gemäß einem Rechte-Rollen-Konzept zu schützen, insofern das der Berichtsinhalt erfordert. Auch dieses Rechte-Rollen-Konzept muss die Anforderungen aus Kapitel 3 erfüllen.

Bei der Nutzung von OneNote ist zu beachten, dass keine sensiblen Informationen aus den Pastoralen Tätigkeiten (z. Bsp. Beichten etc.) oder aus der Mitarbeiterführung gespeichert werden dürfen. Auch ist für Notizen zu Bewerbungen die führende Software der Personalabteilung (aktuell Connectoor) zu verwenden.

Alle Informationen und Dateien sind gemäß der geltenden Löschfristen zu behandeln bzw. rechtzeitig zu löschen.

Es wird den Fachbereichen empfohlen, ein Verzeichnis der Datenverarbeitungstätigkeiten für die jeweils eigenen Prozesse zu erstellen.

Löschungen von Dateien und Informationen in den Microsoft 365 Diensten (OneDrive, SharePoint, OneNote) greifen nicht sofort, da dort (analog zur Arbeit auf dem Desktop) ein Papierkorb im Einsatz ist. Die Dateien und Informationen werden zunächst in den Papierkorb gelegt und dort nach einer bestimmten Zeit gelöscht. Der Nutzer kann den Papierkorb manuell leeren und damit die Löschung beschleunigen.

Die Software OneDrive und Teams (bzw. SharePoint) kann zur Freigabe von einzelnen Dateien, Ordnern oder Ordnerstrukturen sowohl nach intern als auch nach extern verwendet werden. Jeder Nutzer ist verpflichtet, seine Freigaben zu prüfen und mit auslaufendem Verwendungszweck zu beenden. Eine solche Prüfung ist mindestens einmal monatlich durchzuführen.

5.2 E-Mails und E-Mail-Konten

Die E-Mail-Richtlinie aus dem Rundschreiben 10-2024 mit Version vom 27.03.2024 wird mit diesem Dokument aufgehoben.

Für dienstliche Zwecke sind die E-Mail-Adressen der Domains erzbistumberlin.de bzw. ebo-cloud.de zu verwenden. Die private Nutzung dieser E-Mail-Adressen ist nicht gestattet.

Eine E-Mail präsentiert, analog zu einem Brief, sich selbst und den jeweiligen Dienstgeber. Es gilt die Rechtschreibung sowie die Groß- und Kleinschreibung. Eine angemessene Anrede zu Beginn und ein Gruß am Ende sind Teil der E-Mail. Das Verwenden von GROSSBUCHSTABEN und eine Flut von Ausrufezeichen sind unangemessen. Es gilt, sich soweit möglich kurz zu fassen.

Als Standard wird HTML verwendet. Das ist voreingestellt. Text-Mails ermöglichen keine Formatierung, während HTML-Mails mehr Formatierungen erlauben, wobei Standard-Formatierungen den meisten Empfänger-Systemen bekannt sind. Ausnahme sind Bilder, die aus Sicherheitsgründen zumeist manuell vom Empfänger nachgeladen werden müssen.

Eine Änderung der E-Mail-Adresse wegen Namensänderung wird durch Personal-Ressourcen im Rahmen des Workflows veranlasst.

Alle Nutzer gehen sorgsam mit Links und Anhängen in E-Mails um. Die IT des Erzbischöflichen Ordinariats versendet grundsätzlich keine Links (speziell zum Ändern von Passwörtern) für die E-Mail-Adressen.

E-Mails, Links und Anhänge werden systemseitig gescannt und bei Identifizierung mit Hinweisen im Betreff der E-Mail als potenziell gefährlich ausgewiesen. Aufgrund der Schnelligkeit des Internets kann keine 100%-Treffergenauigkeit garantiert werden.

E-Mails von unbekannten Dritten können das Ziel haben, Kontakt herzustellen, um zur Herausgabe von Daten und / oder Geld aufzufordern. Solche Versuche sind zu ignorieren oder zu löschen.

Eine Untersuchung des Absenders ist mit den folgenden Schritten empfohlen, wenn auch nur die einfach gefälschten Absender damit identifiziert werden können:

- E-Mail-Element über Outlook aufrufen und per Doppelklick öffnen
- die Maus über den Namen des Absenders ruhen lassen, bis dieser blau aufleuchtet
- Doppelklick ausführen und die konkrete E-Mail-Adresse ansehen

Im Zweifelsfall hilft der Wechsel des Kommunikationsmittels für eine Kontaktaufnahme mit dem vermeintlichen Absender.

E-Mail-Adressen von Externen dürfen nur für den Zweck verwendet werden, zu dem sie erhoben wurden.

Für Rückfragen im Umgang mit E-Mails und etwaigen Angriffen steht die IT zur Verfügung (siehe 6.).

E-Mails gelten als verbindliches Schriftgut. Sie sind entsprechend der aktuell gültigen Schriftgutverwaltungsordnung im Dokumentenmanagementsystem (DMS – Regisafe) abzulegen - z. Bsp. auf Netzlaufwerken, in Outlook, OneDrive oder Teams gespeicherte Daten und Dokumente bleiben auf Dauer nicht erhalten.

5.2.1 Vorlage Signatur

Die Richtlinien zur Nutzung der Signatur und deren Vorlage befinden sich im Dokument:

Anhang A DNIE E-Mail-Signatur

Anhang B DNIE Anleitung Grafik in Signatur

5.2.2 Vorlage Abwesenheitsnotiz

Bei Abwesenheit ist eine automatische Abwesenheitsnotiz gemäß der folgenden Vorlage einzurichten.

Sehr geehrte Damen und Herren,

bis zum ... bin ich per E-Mail nicht erreichbar.

Ihre E-Mail wird nicht weitergeleitet und daher nicht bearbeitet.

Bitte wenden Sie sich in dringenden Fällen an:

Name

E-Mail-Adresse

Telefonnummer

Signatur

Bei ungeplanter Abwesenheit des Mitarbeiters von mehr als sieben Arbeitstagen greift der direkte Vorgesetzte oder der ständige Urlaubsvertreter in Absprache mit dem Vorgesetzten auf den Active-Directory-Account des abwesenden Mitarbeiters zu, um eine Abwesenheitsnotiz zu setzen.

Abwesenheitsnotizen sind die einzigen automatisch zu versendenden Antworten und können auch über Webmail (<https://webmail.erzbistumberlin.de/>) eingestellt werden.

Sind Mitglieder der Mitarbeitervertretung (MAV) bzw. Schwerbehindertenvertretung (SBV) abwesend, geht der Vorgesetzte oder ständige Urlaubsvertreter in Absprache mit dem Vorgesetzten nur im Beisein eines Mitglieds der MAV bzw. SBV vor.

Ein Termin dafür ist von beiden Seiten unverzüglich zu ermöglichen.

Der Zugriff im Beisein eines Mitglieds der MAV bzw. SBV muss schriftlich dokumentiert werden.

Der Dienstgeber ist nicht berechtigt, E-Mails einzusehen, deren Inhalt sich (nicht zwingend ausschließlich) auf die Tätigkeit der MAV bzw. SBV bezieht. Im Zweifel werden E-Mails vorab von dem anwesenden Mitglied der MAV bzw. SBV gesichtet und explizit zur Einsichtnahme freigegeben oder die Einsichtnahme verweigert.

5.2.3 Rechtsverbindlicher Empfang von E-Mails

Es besteht eine Verweigerung der Zugangseröffnung des Erzbistums Berlin – Erzbischöfliches Ordinariat – für rechtsverbindliche elektronische Nachrichten (gemäß § 3 a Verwaltungsverfahrensgesetz) – mit Ausnahme des besonderen Behördenpostfaches.

Der elektronische Zugang zum Erzbistum Berlin – Erzbischöfliches Ordinariat – insbesondere die Übermittlung elektronischer Dokumente – für eine rechtsverbindliche elektronische Kommunikation mit der Verwaltung im Sinne des § 3 a Abs. 1 Verwaltungsverfahrensgesetz (VwVfG), wird hiermit ausdrücklich zurzeit nicht eröffnet.

Die vorstehende Einschränkung gilt sowohl für die Zugänge per E-Mail-Adressen, für E-Mail-Kontaktformulare als auch für jede Art von Web-Formularen und sonstigen digitalen Zugänge.

Alle anderen bekannten E-Mail-Adressen, sowie personenbezogene E-Mail-Adressen von Mitarbeiterinnen und Mitarbeitern der Verwaltung, stellen keinen offiziellen E-Maileingang dar und bewirken keinen rechtsverbindlichen Zugang.

Eine Benachrichtigung über die Nichtverwertbarkeit im Sinne des § 3 a Abs. 3 Verwaltungsverfahrensgesetz (VwVfG), kann in der Regel nicht erfolgen, da damit ein unverhältnismäßig hoher Aufwand verbunden wäre.

Ausgenommen von der vorstehenden Regelung sind die digitalen Formulare im Antragsportal des Dokumentenmanagementsystems und nicht-personalisierte Funktionspostfächer.

5.2.4 Versand personenbezogener und vertraulicher Daten

E-Mails, die personenbezogene Daten oder vertraulich zu behandelnden Informationen enthalten und extern versendet werden sollen (außerhalb @erzbistumberlin.de / @ebo-cloud.de), sind passwortgeschützt in einem ZIP-Archiv zu verschlüsseln.

Hierfür steht das Verschlüsselungsprogramm 7zip zur Verfügung.

Das Passwort muss über einen gesonderten Kommunikationskanal übermittelt werden.

5.2.5 Erläuterungen zu E-Mail-Komponenten und -Funktionen

Die folgenden Erläuterungen fassen die Komponenten und Funktionen von E-Mails kurz zusammen, um einen Mindestwissensstand zum Thema E-Mails und deren Einsatzmöglichkeiten zu gewährleisten.

„von“-Feld:

Weist den Absender, der E-Mails versendet, aus. Dabei handelt es sich entweder um individuelle E-Mail-Adressen oder um Funktionspostfächer.

„an“-Feld:

Weist den oder die Adressaten aus, der / die die E-Mail erhalten und von denen eine Reaktion erwartet wird.

„cc“-Feld:

cc steht für „Carbon Copy“. Es bedeutet „zur Kenntnis“. Von Adressaten in „cc“ wird keine Reaktion erwartet. Werden Zitate von Dritten per Mail weitergegeben, ist der Zitierte ins CC der E-Mail zu nehmen.

„bcc“-Feld:

bcc steht für "Blind Carbon Copy" und übermittelt die E-Mail ohne Kenntnis der anderen Empfänger an die hier aufgeführten E-Mail-Adressen. Es wird nur genutzt, wenn eine E-Mail an viele Empfänger geschickt wird, die sich nicht kennen, und / oder deren z. Bsp. private E-Mail-Adressen nicht weitergegeben werden dürfen. Es wird der gewählte Verteiler genannt, z.B.: „An die Mitglieder des Pfarreirats“. Dritte über einen Vorgang in „bcc“ zu informieren, so dass die Adressierten das nicht nachvollziehen können, ist zu unterlassen.

Auto-Vervollständigen:

Beim Eingeben der E-Mail-Adressen kann durch die Funktion „Auto-Vervollständigen“ auch irrtümlich ein falscher Adressat ausgewählt werden. Die ausgewählten Adressaten sind daher zu prüfen.

Betreff:

Die Betreffzeile fasst kurz zusammen, worum es in der folgenden E-Mail geht. Sie muss daher möglichst kurz und klar verständlich sein. Häufig wird bei Antworten ein weiteres Thema angeschnitten, sodass Betreffzeilen veralten. Daher ist bei einer erneuten Antwort der Betreff zu überprüfen und ggf. anzupassen.

Dateianhänge:

Für Dateianhänge ist das pdf-Format zu verwenden. Veränderbare Dokumente (Word, Excel, etc.) sind nur zu versenden, wenn die Empfänger damit arbeiten sollen oder berechtigt sind, Änderungen vorzunehmen. Alternativ kann intern auf die entsprechende Datei in Regisafe verwiesen werden.

E-Mail-Anhänge sollten so klein wie möglich sein. Sie dürfen pro E-Mail eine Gesamtgröße von 20 MB nicht überschreiten. Mit einer ZIP-Archivierung kann die Dateigröße reduziert werden. Es ist zu überprüfen, ob der Anhang auch wirklich mitgesendet wird, auch bei der Weiterleitung. Was insbesondere bei schlechtem Netz und/oder mobilen Geräten ein Problem sein kann.

Newsletter:

Für regelmäßige Newsletter an große externe Verteiler wird wegen SPAM-Gefahr, Datenschutz und Handling die Nutzung von Dienstprogrammen vorgeschrieben (CleverReach, etc. aber auch Churchdesk). ZS.6 Medien unterstützt hierzu bei der Umsetzung.

Ordner:

Eine Ordnerstruktur hilft, bei vielen E-Mails den Überblick zu bewahren, den Posteingang zu strukturieren und thematisch verwandte E-Mails zuzuordnen.

Regeln:

Automatische Regeln helfen einen hohen E-Mail-Eingang zu strukturieren und zu sortieren. Sie sollten ab und zu überprüft werden.

Archivieren und Löschen:

Wichtige und relevante E-Mails (Entscheidungen, Aufträge, etc.) werden archiviert (in Abhängigkeit der Möglichkeiten in Papierform oder im Dokumentenmanagementsystem). Was archiviert ist, wird gelöscht. Abgeschlossene Vorgänge werden nur von der verantwortlichen Stelle archiviert.

Ordner "Gelöschte Elemente":

Der Ordner "Gelöschte Elemente" ist regelmäßig in Outlook zu leeren.

5.3 PC-Endgeräte (Desktop / Laptop)

PC-Endgeräte werden Mitarbeitern konfiguriert zur Verfügung gestellt. Die Anschaffung ist ausschließlich über die jeweilige IT-Abteilung bzw. den von der IT beauftragten Dienstleister gestattet. Jeder Mitarbeiter erhält ein PC-Endgerät.

PC-Endgeräte sind achtsam zu nutzen, um deren Langlebigkeit und Werterhalt sicherzustellen. Die aktuellen Geräte halten viele Jahre, wenn sie verantwortungsvoll genutzt werden. Die Geräte dürfen nicht mit Aufklebern o. Ä. versehen werden (abseits für die Inventarisierung durch den Teilbereich R.IV.1).

Ein solches Verhalten wird aufgrund der steuerbasierten Finanzierung der PC-Endgeräte und der möglichen Weitergabe an neue Nutzer erwartet.

Beim Verlassen des Arbeitsplatzes bzw. des Endgeräts ist die Bildschirmsperre einzuschalten. Dafür kann die Tastenkombination Windows-Taste + L verwendet werden.

Insofern Endgeräte für besondere Gelegenheiten zwischengelagert werden, sind diese alle 2 Wochen für 1 Tag im Dienstnetzwerk anzuschließen, damit sie mit den notwendigen Updates versehen werden können.

Es ist unter allen Umständen untersagt, private Datenträger an betriebliche Endgeräte anzuschließen.

Der Einsatz privater Endgeräte ist untersagt. Einzige Ausnahme bildet die Arbeit von zu Hause bzw. Homeoffice und damit die Verwendung einer VPN-Verbindung zur Nutzung von Remote Desktop auf einem privaten Endgerät.

5.4 Smartphones aus dem Mobile Device Management

Smartphones werden Mitarbeitern über das sogenannte Mobile Device Management konfiguriert zur Verfügung gestellt.

Sie enthalten einen technisch eingerichteten Container, der alle betrieblichen Anwendungen und Daten bereitstellt. Elemente des Containers sind mit einem Koffersymbol gekennzeichnet. Betriebliche Daten dürfen nur in diesem geschlossenen Bereich genutzt werden.

Außerhalb des Containers dürfen grundsätzlich nur vertrauenswürdige Apps aus offiziellen App-Stores genutzt werden (Drittanbieter-Apps können Schadsoftware enthalten).

Smartphones sind achtsam zu nutzen, um deren Langlebigkeit und Werterhalt sicherzustellen. Die aktuellen Geräte halten viele Jahre, wenn sie verantwortungsvoll genutzt werden.

Ein solches Verhalten wird aufgrund der steuerbasierten Finanzierung der Smartphones erwartet.

5.5 Künstliche Intelligenz (KI)

Die im Erzbistum Berlin zugelassenen KI-Systeme sind im folgenden Anhang dokumentiert und dürfen nur nach Abschluss der im Anhang aufgeführten KI-Schulung und Einreichen des dazugehörigen Zertifikats an die benannte Kontakt-E-Mailadresse verwendet werden:

- Anhang C DNIE Zugelassene KI-Systeme

Zu jeder Zeit hat der Umgang mit Künstlicher Intelligenz (KI) gemäß dem EU Artificial Intelligence Act zu erfolgen.

Die Nutzung von KI bedarf eines konkreten Einsatzszenarios. KI wird nicht zum Selbstzweck eingesetzt. KI ist ein Werkzeug, das den kirchlichen Auftrag unterstützen soll.

KI-Systeme werden gezielt eingesetzt, um komplexe Aufgaben zu automatisieren, Muster zu erkennen und präzise Analysen durchzuführen.

Die freigegebenen KI-Systeme sind im genannten Anhang aufgeführt. Der Einsatz aller anderen KI-Systeme ist grundsätzlich untersagt.

Bei der Nutzung von KI ist zu beachten, dass die Ergebnisse einer KI nicht immer rechtlich belastbar oder nachvollziehbar sind, weshalb ein verantwortungsbewusster Umgang notwendig ist.

Die Veröffentlichung von KI-generierten Inhalten soll vermieden werden, insofern nicht ausgeschlossen werden kann, dass damit kein Urheberrecht verletzt wird.

Die nachfolgenden 5 Leitlinien sind beim Einsatz von KI zu berücksichtigen:

1.) Der Mensch im Mittelpunkt allen kirchlichen Handelns

KI muss stets zum Wohle des Menschen eingesetzt werden und darf niemals seine Würde oder seine Freiheit einschränken. Der Mensch bleibt das Maß aller Dinge und nicht die Maschine.

2.) Menschliche Beziehungen

KI darf nicht dazu führen, dass menschliche Beziehungen ersetzt oder entwertet werden. Empathie, Mitgefühl und soziale Interaktion sind unverzichtbare Bestandteile menschlichen Zusammenlebens.

3.) Verantwortung und Transparenz

Entwickler, Anwender und Nutzer von KI-Systemen tragen eine hohe Verantwortung. Die Ergebnisse von KI-Systemen müssen transparent (z. Bsp. durch Quellenangaben) sein. KI-generierte Arbeitsergebnisse sind als solche zu kennzeichnen.

Entscheidungen, die unter Einbeziehung von KI-Systemen getroffen werden, müssen transparent gemacht werden. Bevor KI-Ergebnisse in Entscheidungsprozesse integriert werden, sind sie sorgfältig mindestens auf Diskriminierungsfreiheit, inhaltliche Richtigkeit und Vollständigkeit, sowie urheberrechtliche Belange zu prüfen.

Entscheidungen, die auf KI-Ergebnissen basieren, treffen stets Menschen, da nur menschliche Expertise potenzielle Verzerrungen oder unerwartete Ergebnisse identifizieren kann.

Verantwortung darf nicht an KI delegiert werden. Mitarbeitende sind auf die Herausforderungen von KI zu schulen und in ihren digitalen Kompetenzen zu fördern.

4.) Schutz der Privatsphäre

Der Schutz der Daten natürlicher Personen ist ein fundamentales Recht. KI-Systeme dürfen nur mit den wirklich erforderlichen Daten arbeiten und diese müssen sicher gespeichert und verarbeitet werden.

5.) Verantwortung für die Schöpfung

KI soll dazu beitragen, die Welt zu verbessern und nicht sie zu zerstören. Sie soll nachhaltig eingesetzt werden und die Umwelt schützen.

Ein KI-System darf nicht die Diskriminierung Einzelner fördern, Suchergebnisse mit einer unterschwelligen Manipulation versehen, soziale Ungleichheiten schaffen, die Menschenwürde herabsetzen oder gegen grundlegende menschliche oder katholische Prinzipien verstoßen. Ein solches System muss im Zwecke mit der Integrität der katholischen Kirche und der ordnungsgemäßen Durchführung der institutionellen Tätigkeiten der Katholischen Kirche verbunden sein.

Öffentliche KI-Systeme verarbeiten die eingegebenen Daten aus Anfragen zum Anlernen. Die Anlernprozesse führen dazu, dass alte Anfragen für potenziell neue Antworten verwendet werden. Aus diesem Grund ist es nicht gestattet, ausschließlich aus dem dienstlichen Kontext bekannte oder verfügbare Informationen einzugeben.

Dazu gehören Dienst- und Geschäftsgeheimnisse, steuerlich geschützte Informationen und personenbezogene Daten. Auch Inhalte aus Verschlussachen dürfen nicht, auch nicht auszugsweise, eingegeben werden. Die Verwendung von finanziellen Transaktionsdaten, Gesundheitsdaten, Handelsgeheimnissen, vertrauliche interne oder externe Kommunikation, rechtliche Dokumente sowie sicherheitskritische technische Informationen ist untersagt.

Verstöße gegen das Dienstgeheimnis oder besondere Geheimhaltungspflichten können dienst- und strafrechtliche Konsequenzen haben.

Generative KI kann Inhalte erfinden, um eine Anfrage zu beantworten, die auf den ersten Blick plausibel erscheinen. In der Regel wird das nicht gekennzeichnet.

Beim Einsatz generativer KI ist zu beachten, dass die für das Training von KI verwendeten Daten urheberrechtlich geschützte Elemente enthalten können. Es besteht beim Verwenden von KI-generiertem Inhalt das Risiko von Urheberrechtsverletzungen.

Ein Verstoß gegen datenschutzrechtliche Bestimmungen oder Rechte Dritter kann bei der Ergebnisverwendung ebenso stattfinden.

Bei Amtspflichtverletzungen oder Rechtsverstößen haftet das Erzbistum Berlin. Im Falle von Vorsatz oder grober Fahrlässigkeit haftet der Mitarbeitende, der die Eingaben vorgenommen hat.

KI-generierte fotorealistische Bilder oder Videos dürfen für Veröffentlichungen und Webseiten nur mit Freigabe von ZS6 genutzt werden. Sie müssen in der Bildbeschreibung als KI-generiert gekennzeichnet werden – ausgenommen sind grafische Illustrationen.

5.6 Öffentliche Netzwerke

Die Nutzung von öffentlichen und ungesicherten Netzwerken ist untersagt. Insofern ein WLAN nicht passwortgeschützt ist, darf es nicht verwendet werden.

Es empfiehlt sich auf einen Hotspot per Diensthandy auszuweichen.

5.7 Konferenztechnik für Hybride Sitzungen

Im Erzbischöflichen Ordinariat sind die Sitzungsräume St. Hedwig, Bernhard Lichtenberg und Pacellisaal mit Konferenztechnik ausgestattet, die jeweils hybride digitale Sitzungen ermöglicht.

Bei der Nutzung, besonders der ersten, ist zu beachten, dass ausreichend Zeit für die Vorbereitung einer hybriden Sitzung nötig ist. Für die Darstellung von Inhalten ist ein Endgerät nötig, das idealerweise vor der Sitzung mit der Konferenztechnik getestet wird.

Das Ausleihen eines Laptops für unsere Microsoft-Konten oder alternativ eines Laptops für externe Gäste ist am Empfang des Standortes Niederwallstraße möglich.

Anhang D Anleitung St. Hedwig

Anhang E Anleitung Pacellisaal



6 Support

Nachfolgend eine Übersicht der Support-Angebote für die IT-Infrastruktur:

IT-Infrastruktur im Erzbischöflichen Ordinariat samt Nebenstellen

R.IV.1 Digitalisierung

Tel. : +49 30 / 32 68 4 333

E-Mail. : it.helpdesk@erzbistumberlin.de

Standardisierte IT-Infrastruktur der Pfarreien

Cancom GmbH

Öffnungszeiten : Mo – So (inkl. Feiertage) 7:00 bis 18:00 Uhr

Tel. : +49 911 / 64 19 49 65 57

E-Mail : servicedesk@cancom.de

Churchdesk

Churchdesk GmbH

Öffnungszeiten : Mo – Fr 9:00 bis 12:30 und 13:00 bis 15:00 Uhr

Tel. : +49 30 568373604

E-Mail : support@churchdesk.com

7 Schulungen

Für jeden Mitarbeiter im Erzbistum Berlin ist die Teilnahme an der Datenschutzs Schulung über ZS.8 verpflichtend. Die entsprechenden Teilnahmenachweise sind unaufgefordert bei ZS 8 vorzulegen.

Jeder Nutzer von Informationstechnologie der vom Teilbereich R.IV.1 verantworteten Informationstechnologieinfrastruktur sowie der darin genutzten Fachanwendungen muss an der Phishing- und Cybersicherheitsschulung über die Plattform perseus.de teilnehmen. Eine Anmeldung kann über perseus@erzbistumberlin.de angefragt werden.

Jeder neue Mitarbeiter erhält eine Einführungsschulung in Regisafe. Zusätzliche darauf aufbauende Schulungen oder Auffrischungen können jederzeit im Teilbereich R.IV.1 Digitalisierung angefragt werden.

Schulungsunterlagen und –videos zur Nutzung von MS Teams und MS365, Windows 11 sowie der Barrierefreiheit in Windows 11 liegen in MS Teams im Team Erzbischöfliches Ordinariat Berlin im Kanal Allgemein im Reiter Dateien im Ordner Schulungsunterlagen.

Nutzer von KI müssen eine Schulung für KI gemäß den Vorgaben des EU AI Act vor der Nutzung der KI absolvieren und das zugehörige Zertifikat abgeben. Die genauen Anforderungen sind dem folgenden Anhang zu entnehmen:

- Anhang C DNIE Zugelassene KI-Systeme

8 Notfallmanagement

Bei der Nutzung der IT-Infrastruktur kann es zu verschiedenen Formen von Notfällen kommen. Beim Eintreten des jeweiligen Szenarios ist gemäß den folgenden Anweisungen zu handeln.

Für hier etwaig nicht aufgeführte Szenarien wird ein verantwortungsvoller Umgang mit der entsprechenden Situation nebst einer umfangreichen Kommunikation mit dem Vorgesetzten erwartet.

Versehentlich Passwort weitergegeben

Insofern ein Nutzer versehentlich das Passwort weitergibt (z. Bsp. durch Phishing) ist sofort das Passwort neu zu vergeben und der Vorgesetzte sowie die IT-Abteilung zu informieren.

Versehentlich auf zwielichtigen Link geklickt

Sollte ein Nutzer versehentlich auf einen Link klicken, der sich als schädlich herausstellt, ist das Endgerät sofort vom Netzwerk / Internetzugriff zu trennen.

Im Anschluss ist der Vorgesetzte und die zuständige IT-Abteilung zu kontaktieren.

Weitergabe personenbezogener Daten

Sollten personenbezogene Daten widerrechtlich weitergegeben oder gespeichert worden sein, ist umgehend der Vorgesetzte und ZS. 8 zu informieren. ZS. 8 übernimmt die Kommunikation mit dem Datenschutzbeauftragten und der Datenschutzaufsicht.

Defekt / Diebstahl IT-Infrastruktur-Komponente

Bei einem Defekt oder einem Diebstahl einer IT-Infrastruktur-Komponente (PC-Endgerät, Smartphone, Netzwerkgeräte etc.) ist sofort der Vorgesetzte und die zuständige IT-Abteilung zu informieren.

Nicht-Nutzung von PC-Endgeräten / Smartphones

PC-Endgeräte, die nicht mehr verwendet werden, sind umgehend in der zuständigen IT-Abteilung abzugeben. Smartphones werden an den Teilbereich Allgemeine Dienste zurückgegeben.



9 Anhänge

- Anhang A DNIE E-Mail-Signatur
- Anhang B DNIE Anleitung Grafik in Signatur
- Anhang C DNIE Zugelassene KI-Systeme
- Anhang D DNIE Anleitung St. Hedwig
- Anhang E DNIE Anleitung Pacellisaal

Versionierung

Das Kapitel Versionierung soll über die Neuerungen sowie Änderungen der jeweils neuen Version hinweisen, um das Nachvollziehen der Änderungen zu optimieren.

1.1.:

Rückmeldung der MAV vom 6. November 2025:

Die über die Kommentarfunktion eingereichten Anmerkungen wurde alle umgesetzt.

Der Text 5.2.3 ist von ZS. 8 formuliert und freigegeben worden.

Die Nutzung von öffentlichen Netzwerken ist aufgrund des hohen Sicherheitsrisikos nicht gestattet. Die Empfehlung zur Hotspot-Nutzung per Diensthandy wurde hinzugefügt. Das Ganze ist unabhängig von VPN.

2. Benutzerkonten:

Es wurde ergänzt, dass E-Mailadressen nicht auf private E-Mailadressen weitergeleitet werden dürfen.

4. Datenmanagement:

Ein Absatz wurde ergänzt, der die Nutzung der Informationen bzw. Daten in Administrationsoberflächen auf den Support-Zweck einschränkt.

4.2 Absatz „Öffentlich“:

Der Hinweis zum Schutzbedarf öffentlicher Informationen wurde angepasst, da auch öffentlich verfügbare Informationen und personenbezogene Daten den Vorgaben des Datenschutzes unterliegen.

4.4 Transkription

Der Passus wurde vollständig überarbeitet. Transkription bedarf der expliziten Zustimmung durch die Teilnehmer. Die Freiwilligkeit wurde betont und auf das Recht des Widerrufs hingewiesen sowie die Methodik erklärt.

5.1 Software und Fachanwendungen

Es wurde ein Verbot zur Leistungs- und Verhaltenskontrolle unter Einsatz bestimmter Software aufgenommen, insofern keine gültige Dienstvereinbarung verabschiedet wurde, die die Leistungs- und Verhaltenskontrolle regelt.

Ein Absatz zur möglichst anonymisierten Nutzung von MS Forms wurde hinzugefügt, der auch auf das Risiko der Eingaben bei Freitextfeldern hinweist. Die Nutzung von MS Project wurde auch in Bezug auf Freitextfelder eingeschränkt.

Die Nutzung von PowerBI wurde analog zur KI-Nutzung dahingehend eingeschränkt, dass automatisiert erzeugte Berichte nicht ohne menschliche Plausibilitätsprüfung verwendet werden dürfen, und einem dem Inhalt angepasstem Rechte-Rollen-Konzept entsprechend.

Ein Datenschutzhinweis zur Vermeidung der Speicherung sensibler Daten bei der OneNote-Nutzung ist eingearbeitet worden.



Eine Erklärung zum Papierkorb-System in den MS 365 Diensten wurde ergänzt.

Alle Nutzer sind verpflichtet, die Freigaben mindestens einmal monatlich zu überprüfen.

5.5 Künstliche Intelligenz

Es wurde ergänzt, dass die im Anhang veröffentlichen KI-Systeme nur nach Absolvieren der dort aufgeführten Schulung und Einreichen des dazugehörigen Zertifikats verwendet werden dürfen.

Ein Hinweis wurde aufgenommen, der eine Veröffentlichung von KI-Inhalten untersagt, wenn ein Verletzen des Urheberrechts in Bezug auf die generierten Inhalte nicht ausgeschlossen werden kann.

Zusammenfassung

Für einen Schnellüberblick der wichtigsten Inhalte dieses Dokuments wurde eine KI-generierte und im Anschluss manuell überprüfte Zusammenfassung beigefügt.

Anhänge

Die Anhänge sind erweitert und in der Reihenfolge, inhaltlich passend, aufgelistet.

Zusammenfassung

Diese Zusammenfassung ist KI-generiert.

Das Dokument beschreibt umfassende Richtlinien und Vorgaben für den sicheren und gesetzeskonformen Umgang mit Informationstechnologie im Erzbistum Berlin. Es regelt Benutzerkonten, Datenmanagement, IT-Komponenten, E-Mail-Nutzung, Künstliche Intelligenz sowie Notfallmanagement und Support.

- **Geltungsbereich und Verantwortung:** Die IT-Abteilung des Erzbischöflichen Ordinariats ist für die IT-Infrastruktur und Fachanwendungen verantwortlich, die in verschiedenen Dienststellen und Pfarreien genutzt werden. Änderungen an der IT-Infrastruktur bedürfen der Zustimmung der zuständigen Bereichsleitungen. Die Nutzung der IT darf keine rechtswidrigen oder beleidigenden Inhalte umfassen. Verstöße können zur Sperrung von Konten oder Geräten führen.
- **Personalisierte Benutzerkonten:** Nutzer erhalten personalisierte Konten mit den Domains erzbistumberlin.de oder ebo-cloud.de, geschützt durch starke Passwörter und Multi-Faktor-Authentifizierung. Passwörter dürfen nicht weitergegeben oder in Browsern gespeichert werden. Private Nutzung der Konten und Nutzung auf privaten Geräten über office.com sind untersagt. Für Homeoffice steht VPN mit Remote-Desktop-Zugriff zur Verfügung.
- **Rechte- und Rollenkonzepte:** Zugriffsrechte werden nach dem Prinzip der Notwendigkeit vergeben und regelmäßig überprüft. Unberechtigter Zugriff auf vertrauliche oder personenbezogene Daten ist zu melden. Änderungen im Personalbestand müssen zeitnah im Rechte- und Rollensystem erfasst werden. Fachanwendungen sind für eigene Rechtekonzepte verantwortlich.
- **Datenmanagement und Datenschutz:** Der Umgang mit Daten erfolgt gemäß dem Kirchlichen Datenschutzgesetz (KDG). Dienstliche Daten sind ausschließlich auf Dienstgeräten oder -umgebungen zu speichern; private Datenträger sind verboten. Personenbezogene Daten umfassen alle identifizierbaren Informationen natürlicher Personen und sind besonders zu schützen. Daten werden in öffentlich, intern und vertraulich klassifiziert. Gesicherte Speicherorte mit Backup sind Netzlaufwerke, Regisafe, OneDrive und MS Teams.
- **Umgang mit IT-Komponenten:** Private Nutzung von Software und Fachanwendungen ist untersagt. Softwareeinsatz erfordert Genehmigungen und Datenschutzfreigaben. E-Mail-Adressen der genannten Domains sind dienstlich zu verwenden; private Nutzung ist verboten. E-Mails gelten als verbindlich, wenn sie im Dokumentenmanagementsystem abgelegt werden.
- **E-Mail-Richtlinien:** E-Mails müssen formell korrekt sein und HTML als Standardformat nutzen. Anhänge sollten vorzugsweise im PDF-Format und unter 20 MB sein. Automatische Abwesenheitsnotizen sind bei Abwesenheit einzurichten. Externe E-Mail-Adressen dürfen nur zweckgebunden verwendet werden.
- **Künstliche Intelligenz (KI):** Der Einsatz von KI-Systemen ist auf zugelassene Anwendungen beschränkt und muss dem EU Artificial Intelligence Act entsprechen. KI dient als Werkzeug zur Unterstützung des kirchlichen Auftrags, wobei der Mensch stets im Mittelpunkt steht. Es gelten fünf Leitlinien: Menschlichkeit, menschliche Beziehungen, Verantwortung und Transparenz, Datenschutz und Nachhaltigkeit. Vertrauliche und personenbezogene Daten dürfen nicht in



öffentliche KI-Systeme eingegeben werden. KI-generierte Inhalte sind entsprechend zu kennzeichnen.

- **IT-Support:** Für die IT-Infrastruktur im Ordinariat und Nebenstellen sowie in den Pfarreien stehen unterschiedliche Supportstellen mit Kontaktdaten und Öffnungszeiten zur Verfügung.
- **Schulungen und Notfallmanagement:** Datenschutz- und Cybersicherheitsschulungen sind verpflichtend. Neue Mitarbeiter erhalten Einführungsschulungen zu Fachanwendungen. Im Notfall, etwa bei Passwortweitergabe, Klick auf schädliche Links, Datenweitergabe oder Geräteverlust, sind sofort Vorgesetzte und IT zu informieren und entsprechende Maßnahmen zu ergreifen.