Dienstvereinbarung über
(I.) die Einhaltung des Datenschutzes/der Datensicherheit und
(II.) die private Nutzung von elektronischen Kommunikationssystemen

Zwischen dem

Ev.-luth. Kirchenkreisverband (…),
vertreten durch den Kirchenkreisverbandsvorstand

und

der Mitarbeitervertretung
des Ev.-luth. Kirchenkreisverbandes (…)

wird folgende Dienstvereinbarung geschlossen:

I. Datenschutz / Datensicherheit

1. Datenschutz

Persönliche und personenbezogene Informationen, über die in dienstlichen Zusammenhängen Kenntnis erlangt wird, dürfen nicht zu privaten Zwecken genutzt oder an Dritte zur Nutzung außerhalb der dienstlichen Zweckbestimmung weitergegeben werden.

Die gesetzlichen Bestimmungen des Urheberrechts sind zu beachten. Das heißt, dass vor der Weitergabe und Verbreitung von Informationen (Schriftstücke, Bilder, Ton- und Textdokumente, u.a.) zu klären ist, ob diese urheberrechtlich geschützt sind (insbesondere "Recht am eigenen Bild"). Im Zweifelsfall ist eine Erlaubnis/ Genehmigung des Rechtsinhabers einzuholen oder aber auf die Verbreitung der Information zu verzichten.

2. Datensicherheit - allgemein

Die Mitarbeitenden sind angehalten, Daten nicht auf den lokalen Festplatten und dem Desktop zu speichern, sondern auf der zentralen Datenablage (Server).

Benutzernamen und Passwörter sind vertraulich zu behandeln und dürfen nicht an Dritte weitergegeben werden.

Bei jedem Verlassen des Arbeitsplatzes sind die Systeme vor unberechtigtem Zugriff bzw. unberechtigter Einsichtnahme zu schützen. Sofern hierzu das System nicht aktiv (durch gleichzeitiges Drücken der Windows-Taste und der L-Taste) durch den Mitarbeitenden gesperrt wird, erfolgt nach 10-minütiger Nichtbenutzung des Systems eine automatisierte Sperre.
Der Mitarbeitende hebt die Sperre jeweils durch Eingabe des Passwortes auf.

3. Datensicherheit — E-Mails, Internet

E-Mails mit angehängten Dateien, die ausführbar sind (z.B. "*.exe") oder ausführbare Bestandteile haben (z.B. Makros) und deren Zweck oder Herkunft nicht eindeutig zuzuordnen ist, sind mit Vorsicht zu behandeln, da diese Anhänge evtl. Schaden auf der Hardware (Arbeitsplatzcomputer, Handy, Smartphone) und/ oder im Netzwerk anrichten können.

E-Mails, die unaufgefordert eingehen und von unbekannten Absendern stammen (insbesondere Werbe-, Spam-, Junk-Mail), sollten in der Regel nicht beantwortet und sofort ge-

löscht werden, wenn kein dienstlicher Zusammenhang erkennbar ist. Sicherheitshalber ist diese Mail auch im Papierkorb (z.B. Ordner: "Gelöschte Elemente") zu löschen. Insbesondere dürfen aufgrund solcher E-Mails keine Adress-, Konto- oder Zugangsdaten mitgeteilt oder Informationen, die dem Datenschutz unterliegen, weitergegeben werden.
Im Zweifelsfall ist die IT-Stabssteile des Kirchenamtes (IT-KA) vor dem Öffnen solcher Anhänge zu befragen.

Das Herunterladen von Dateien ist nur in Absprache mit der IT-KA erlaubt. Ausgenommen hiervon sind lediglich PDF- (Postscript-Data-Files) und Office-Dateien sowie Arbeitshilfen von der Webseite der Landeskirche. Enthalten heruntergeladene Dateien ausführbare Bestandteile (z.B. Makros), gelten die gleichen Vorsichtsmaßnahmen wie für E-Mail-Anhänge.

4. Datensicherheit - fremde Hard-/Software

Externe Datenträger wie USB-Sticks, externe Festplatten, Speicherkarten etc. unterliegen der Verwaltung, Zuteilung und ggf. Verschlüsselung durch die IT-KA und dürfen erst nach ausdrücklicher Freigabe eingesetzt werden.

Das Laden, Installieren und Betreiben von Apps auf dienstlichen Smartphones, die nicht dem ursächlichen Verwendungszweck dienen, ist nicht gestattet.

5. Einhaltung des Urheberrechts

Software, die in der IT-KA installiert ist, darf nicht kopiert werden, es sei denn, dass sie ausdrücklich von der IT-KA zum Kopieren freigegeben wurde. Für Eigenentwicklungen der IT-KA kann bei der IT-KA eine Kopiererlaubnis beantragt werden. Es gelten die gesetzlichen Bestimmungen des Urheberrechts. Dekompilierungen sind unzulässig. Bei der Nutzung von Software, die von der IT-Stabsstelle zur Verfügung gestellt wird, sind die Lizenzbestimmungen des Softwarelieferanten einzuhalten. Diese können in der IT-KA eingesehen werden

II- Private Nutzung von elektronischen Kommunikationssystemen

6. Grundsatz

Die Nutzung der Kommunikationssysteme (Internet, E-Mail, Smartphones, u.a.) hat ausschließlich zu dienstlichen Zwecken zu erfolgen. Die Nutzung zu privaten Zwecken ist nur in begründeten Ausnahmefällen gestattet.

7. Zugangsbeschränkungen

Untersagt ist die Nutzung von (Free) -Webmail-Anbietern, Chat-Diensten (z.B. Facebook, Twitter, u.a.), Spiele-Diensten, Online Video-Plattformen und Online-Shops und vergleichbaren Portalen.

Der Zugriff auf diese Online-Dienste ist gesperrt, kann aber im Einzelfall auf Antrag bei der Abteilungsleitung durch die IT-KA freigeschaltet werden.

Unzulässig ist jede Nutzung der Kommunikationssysteme, die:
(a) gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt oder
(b) für den Arbeitgeber geschäftsschädigende oder in sonstiger Weise beleidigende, verleumderische, verfassungsfeindliche, rassistische, sexistische oder pornographische Inhalte aufweist.

Sofern durch diese Regelung private Nutzungen von Kommunikationssystemen eingeräumt werden, unterliegen sie dem jederzeitigen Widerrufsrecht durch den Arbeitgeber.

8. Nutzungserfassung

Die IT-Systeme und die Fachanwendungen in der IT-KA protokollieren automatisiert alle relevanten Systemaktionen.

Fallen bei der Nutzung von Kommunikationssystemen (z.B. E-Mail, Internet, Smartphones sowie mobile Kommunikationssysteme, die vom Arbeitgeber eingerichtet wurden (z.B. Homeoffice) u.a.) personenbezogene Daten an, werden diese grundsätzlich nicht zu einer Leistungs- und/oder Verhaltenskontrolle verwendet. Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen Betriebs von Kommunikationssystemen erhoben und gespeichert werden, unterliegen der besonderen Zweckbestimmung nach §24 Absatz 7 DSG-EKD.
Die erfassten Protokoll- und Verbindungsdaten werden ausschließlich zum Zweck der Gewährleistung der Systemsicherheit, zur Steuerung und Optimierung der Lastverteilung im Netzwerk, für die Analyse und Korrektur von technischen Fehlern und Störungen sowie zur Missbrauchskontrolle und bei Verdacht auf Straftaten unter Einbeziehung der MAV verwendet.
Eine stichprobenartige Kontrolle durch die Amtsleitung unter Einbeziehung der MAV ist möglich.
Das unter Ziffer 6 beschriebene Verbot der Privatnutzung sowie die Notwendigkeit einer Kontrolle führt zur Nichtanwendbarkeit der gesetzlichen Regelungen über das Fernmeldegeheimnis gem. § 88, Abs. 2 TKG.

9. Nutzungsmissbrauch

Zum Missbrauch gehört u.a.:

- die Weitergabe des eigenen Passwortes
- der Versuch, ohne Zustimmung des Betreffenden dessen Daten zu verändern oder zu kopieren.
- die Installation von Programmen, sofern nicht ausdrücklich eine Sondererlaubnis vorliegt.
- die bewusste Installation und Verbreitung von Computerviren.
- die Benutzung von Spielen.
- das Kopieren von Daten aus weltweiten Netzen, die keiner dienstlichen Anforderung entsprechen. Für Schäden, die durch grobe Fahrlässigkeit entstehen, kann der Verursacher haftbar gemacht werden.
- die Benutzung von E-Mail-Verteilern für nichtdienstliche Zwecke.

10. Geltungsdauer

Diese Dienstvereinbarung tritt am Tag nach der Unterzeichnung in Kraft.
Sie kann mit einer Frist von sechs Monaten zum Ende eines Monats gekündigt werden.

(…), (…),

(Kirchenkreisverbandsvorstand) (Mitarbeitervertretung)