Dienstanweisung für die Nutzung des IT-Systems

in der _____

1. Vorwort

Über das lokale Netz unserer Einrichtung wird ein Internetzugang bereitgestellt, der einem Teil der MitarbeiterInnen als Arbeitsmittel zur Erfüllung ihrer dienstlichen Aufgaben eingerichtet wird. Hierdurch sind Sie für Dritte von Außen erreichbar. Darüber hinaus können in berechtigten Fällen Informationen aus dem dienstlichen Bereich über das Internet an andere übermittelt werden.

Das Internet sieht grundsätzlich keinerlei Maßnahmen zur Sicherstellung der Integrität, Vertraulichkeit und Authentizität der übertragenen Daten vor. Das gilt besonders auch für E-Mail. Bei dem normalen Versand solcher Nachrichten gibt es keine eindeutigen Feststellungsmöglichkeiten hinsichtlich

- der Person des Absenders (Authentizität),
- des Umstandes, dass der Inhalt der Nachricht auf dem Transportweg nicht verändert wurde (Integrität),
- und der im Hinblick auf § 203 StGB (Schweigepflicht) und das kirchliche Seelsorgegeheimnis erforderliche Vertraulichkeit der übermittelten Informationen.

Daher sind bei der Benutzung zusätzliche Datensicherheits- und Datenschutzmaßnahmen anzuwenden. Sie sind aufgefordert, hieran in verantwortungsvoller Weise mitzuwirken.

Die Auswahl der zu ergreifenden Sicherheitsmaßnahmen wurde durch die Leitung der Einrichtung getroffen und durch die EDV-Technik vorbereitet. Diese Maßnahmen können aber nur zu einem gewissen Teil von sich aus ihre Wirksamkeit entfalten. Ein ganz entscheidender Faktor zur Gewährleistung und Verbesserung des vorhandenen Sicherheitsniveaus ist deren konsequente und gewissenhafte Anwendung in der täglichen Arbeit durch jeden Einzelnen.

Daher sind die Kenntnis dieser nachfolgenden Regelungen und deren Einhaltung durch jeden einzelnen berechtigten Mitarbeiter eine wesentliche Voraussetzung für die Gewährleistung der Sicherheit dieses Kommunikationsmittels und unserer Dienststelle.

Jede Missachtung und Nichteinhaltung dieser Regelungen gefährdet nicht nur die Vertraulichkeit, Verfügbarkeit und Integrität der von Ihnen auf Ihrem eigenen DV-System unmittelbar be- und verarbeiteten Daten, sondern es wird dadurch auch die Vertraulichkeit, Verfügbarkeit und Integrität aller sonstigen Daten unseres Hauses gefährdet.

Diese Benutzerrichtlinien stehen ergänzend zu den sonstigen geltenden Regelungen und Vorschriften bzgl. der Anwendung von Informationstechnik und für den Umgang mit personenbezogenen oder sonstigen schutzwürdigen Daten.

2. Regelungen

2.1. Verantwortung

Sie sind als berechtigter Mitarbeiter in Ihrem Zuständigkeitsbereich verantwortlich für die vollständige und korrekte Anwendung der jeweils geltenden Regelungen, Anweisungen und Vorschriften zur Gewährleistung von Datenschutz und Datensicherheit

Sie sind als berechtigter Mitarbeiter insbesondere zuständig und verantwortlich für die in Ihrem Zuständigkeitsbereich liegende wirksame Anwendung der vorgesehenen und vorhandenen Datensicherheitsmaßnahmen, wie beispielsweise die Nutzung der installierten Schadensbekämpfungssoftware, Nutzung von sicheren Passworten und Entscheidung über die Vertraulichkeit der übermittelten Informationen.

2.2. Nutzung des Internet

Das Einbringen und der Betrieb von privater Hard- und/oder Software (auch für die Nutzung des Internets) in das lokale Netz sind unzulässig, weil dadurch Sicherheitslücken eröffnet werden können und eventuell unkontrollierbare und ungesicherte Übergänge in das lokale Netz geschaffen werden.

Für die Nutzung des Internets sind die folgenden Bedingungen zu beachten:

- Genutzt werden dürfen ausschließlich die Internetdienste, die in ihrem Nutzerprofil festgelegt sind.
- Werden darüber hinaus weitere Dienste benötigt, ist deren Zulassung bei bei der Systemverwaltung zu beantragen. Nicht mehr benötigte Dienste sind der EDV-Abteilung zur Änderung Ihres Berechtigungsprofils umgehend mitzuteilen.
- Die Nutzung der erlaubten Dienste ist ausschließlich zu dienstlichen Zwecken und im ausdrücklich erlaubten Umfang zur Erledigung Ihrer Aufgaben gestattet. Ihre Nutzung zu privaten Zwecken ist untersagt.
- Das Ausprobieren, ob weitere Dienste als die ausdrücklich erlaubten zur Verfügung stehen und evtl. genutzt werden können, ist unzulässig.
- Das Ausprobieren, das Ausforschen und die Benutzung fremder Zugriffsberechtigungen (ggf. Aufzählung wie z.B. Benutzerkennungen, Passworte, persönlicher Identifikationsausweise oder Verweis auf entsprechende sonstige Regelungen und Vorschriften) und sonstiger Authentifizierungshilfsmittel (ggf. Aufzählung wie z.B. Chipkarten, Magnetkarten, usw. oder Verweis auf entsprechende sonstige Regelungen und Vorschriften) ist unzulässig.
- Die Weitergabe und das Zurverfügungstellen von eigenen Benutzerkennungen und sonstigen Authentifizierungshilfsmitteln für eine Benutzung durch Dritte sind unzulässig. Es wird ausdrücklich darauf hingewiesen, dass in einem derartigen Fall aus den Protokolldaten Ihre Identität hervorgeht. Jegliche Aktivität - auch unzulässige - durch diesen Dritten wird also Ihnen zugeschrieben.
- Das Ausführen von Programmen oder von ausführbarem Programmcode, die aus dem oder über das Internet beschafft wurden, ist ohne vorherige Prüfung und Freigabe durch die Systemverwaltung untersagt. Hierdurch soll das Risiko des Einschleppens von Schadenssoftware im lokalen Netzwerk reduziert werden.

2.3. Verschlüsselung der Datenübertragung (Kryptographische Schutzmaßnahmen)

Die Übertragung von personenbezogenen Daten sowie weiteren vertraulichen Informationen über das Internet ist, zur Gewährleistung der Authentizität, Integrität und Vertraulichkeit, ausschließlich in verschlüsselter Form zulässig.

Hierzu wird Ihnen

☐ ein S/MIME-Zertifikat der Zertifizierungsstelle _____
☐ ein Schlüsselpaar für PGP
☐ das ZIP-Programm _____

zur Verfügung gestellt. Die erforderliche technische Installation erfolgt durch die Systemadministration. Eine fachliche Anweisung zur Benutzung hierfür haben Sie erhalten.

Die Beurteilung, ob derartige Daten zur Übertragung vorliegen, erfolgt durch Sie als Absender selbst. Dabei ist ein strenger Maßstab anzulegen. Diese Daten sind dann mit dem vorgenannten spezifischen Hilfsmittel durch Sie vor dem Versand zu verschlüsseln. Gleiches gilt für die Anwendung und Nutzung der elektronischen Signatur.

2.4. Sicherheitsrelevante Ereignisse

Alle sicherheitsrelevanten Ereignisse (z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung, usw.) sind sofort an dem Systemadministrator zu melden. Überlassen sie ihm die Überprüfung der Angelegenheit! Unternehmen Sie keine eigenen Aufklärungsversuche, da hierdurch eventuell wertvolle Hinweise und Spuren verwischt werden oder verloren gehen könnten.

Systemadministrator ist Frau/Herr _____, Tel.: _____

2.5. Unzulässige Nutzungen

Sie haben sich bei der Nutzung des Internets so zu verhalten, wie es von kirchlichen Mitarbeitern im Sinne der "Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse" erwartet werden kann. Daher sind folgende Internetnutzungen nicht mit Ihrem Dienst vereinbar:

- Das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen.
- Das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, volksverhetzenden, sexistischen, gewaltverherrlichenden, oder pornografischen Äußerungen oder Abbildungen.
- Das Abrufen oder Verbreiten von Inhalten, die kirchenfeindlich ausgerichtet sind und die Glaubwürdigkeit der Kirche und der Einrichtung gefährden.

2.6. Protokollierung und Kontrollen

Jeder Datenverkehr innerhalb des lokalen Netzes und zwischen dem lokalen Netz und dem Internet kann/wird einer automatischen/vollständigen/gezielten Protokollierung unterliegen.

Sofern eine Nutzung der Dienste zu privaten Zwecken erfolgt ist, so unterliegt auch diese Nutzung der Protokollierung gemäß den nachfolgenden Maßgaben:

- Die Protokolle werden für den Zeitraum von drei Monaten aufbewahrt und bei Verdacht auf einen Sicherheitsverstoß durch eigens hierfür Berechtigte (z.B. Datenschutzbeauftragter, Sicherheitsteam) ausgewertet.
- Die Protokolldaten dienen ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebes. Sie werden nicht für Zwecke der Leistungskontrolle verwendet.
- Die Einhaltung dieser Richtlinien kann durch die Systemverwaltung stichprobenartig und anlassbezogen kontrolliert werden.

3. Sanktionen

Verstöße gegen diese Benutzerrichtlinien und die sonstigen Regelungen und Vorschriften bzgl. der Anwendung der Informationstechnik und bzgl. des Umgangs mit personenbezogenen Daten können dienst- und arbeitsrechtliche sowie strafrechtliche Konsequenzen haben. Sie können auch Grund für eine fristlose Kündigung sein.

4. Erklärung

Der Benutzer bestätigt die Kenntnisnahme der vorstehenden Regelungen.

Er erklärt, die vorstehenden Regelungen zu beachten.

Er erklärt für den Fall, dass eine private Nutzung der bereitgestellten Dienste gestattet ist, seine Einwilligung in die beschriebene Protokollierung (Anmerkung: für den Fall der Einwilligungsverweigerung ist die Nutzung der bereitgestellten Dienste für private Zwecke zu untersagen).

Er bestätigt durch die nachfolgende Unterschrift den Erhalt eines Abdruckes dieser Benutzerrichtlinie.

Eine Ausfertigung erhält darüber hinaus der betriebliche Datenschutzbeauftragte, eine weitere Ausfertigung wird zum Personalakt genommen.

_____ _____

(Ort, Datum) (Unterschrift)