Dienstanweisung zur Nutzung von Internet, E-Mail, Fernmeldeeinrichtungen, etc.

1. Gegenstand und Geltungsbereich

Diese Vereinbarung regelt die Grundsätze für Einsatz und Anwendung elektronischer Kommunikationssysteme und den Betrieb und die Nutzung der informationstechnischen Infrastrukturen bei der Evangelischen Altenhilfe gGmbH Ludwigshafen und gilt für alle Beschäftigten, die mit solchen Systemen arbeiten.

Diese Vereinbarung umfasst unter anderem das E-Mail-System, den Zugang zum Internet und das geschäftliche Netz und die Informationstechnik der Einrichtungen.

2. Zielsetzung

Ziel dieser Vereinbarung ist es, den Einsatz einer leistungsfähigen und zeitgemäßen Technik und die in absehbarer Zukunft erforderlichen Neuerungen offener informations- und kommunikationstechnischer Infrastruktur mit dem Schutz der Persönlichkeitsrechte für die betroffenen Mitarbeiterinnen und Mitarbeiter zu verbinden.
Die zur Verfügung gestellten Dienste dienen der Information und Kommunikation im Interesse der Evang. Altenhilfe gGmbH, Ludwigshafen. Bei ihrer Nutzung muss die Sicherheit des IT-Systems bzw. Firmennetzes gewährleistet bleiben.

3. Zulässigkeit der Nutzung

(1) Das E-Mail-System wird nur für die geschäftsmäßige Nutzung zur Verfügung gestellt, jegliche private Nutzung ist untersagt.

(2) Die Internetnutzung dient ausschließlich geschäftsmäßigen Zwecken.

(3) Über geschäftliche E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Firmenpost behandelte E-Mails sind den betreffenden Beschäftigten unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.
Die betreffenden Beschäftigten informieren nach Kenntnisnahme den Absender der privaten E-Mails, dass die geschäftlichen E-Mail-Adressen nicht für private Zwecke genutzt werden dürfen. Die privaten E-Mails sind danach unverzüglich zu löschen.

(4) Dokumente, die personenbezogene oder andere sensible Daten beinhalten, dürfen nicht unverschlüsselt übertragen werden oder sollten zumindest kennwortgeschützt sein.

(5) Das Abrufen und Ausführen von Dateien oder Programmen aus und im Internet ist nur von und bei den von der Geschäftsführung bekannt gegebenen Anbietern gestattet, soweit deren Inhalte für den innerbetrieblichen Gebrauch benötigt werden. Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden. Das Ausführen von aktiven Inhalten (z. B. Makros) in heruntergeladenen Dokumenten ist nur bei als vertrauenswürdig gekennzeichneten Anbietern gestattet. Die Einstellungen in die zugehörigen Anwendungen werden von der Geschäftsführung durchgeführt oder beauftragt.
(6) Das Abrufen von Kosten verursachenden Informationen oder Inhalten aus dem Internet ist von der Geschäftsführung zu genehmigen.

(7) Das Anrufen von Kosten verursachenden Sonder-, Service oder ausländischen Rufnummern ist von der Geschäftsführung zu genehmigen.

(8) Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen über sogenannte Remote-Anwendungen bzw. Terminal-Emulationen sind grundsätzlich nicht zugelassen. Sollte Bedarf für Remote.Zugriffe bzw. Terminal-Emulationen bestehen, sind diese bei der Geschäftsführung unter Angabe der Gründe zu beantragen.

(9) Die Internet-Telefonie und Bildtelefonie sind grundsätzlich nicht zugelassen. Ausnahmen für den betrieblichen Gebrauch sind bei der Geschäftsführung zu beantragen und nur mit der dafür zur Verfügung gestellten Software zulässig.

(10) Für den Fall einer Abwesenheit (Urlaub, Krankheit, Fortbildung, etc.) hat der Mitarbeiter eigenverantwortlich eine automatisierte Antwort an den Absender eingehender E-Mails einzurichten, die den Absender über ihre Abwesenheit informiert und einen Hinweis auf den zuständigen Vertreter und dessen Telefonnummer enthält. Gleichwohl wird eine Weiterleitung der E-Mails an die Vertretung eingerichtet.
Im Krankheitsfall muss der Arbeitnehmer seinen Vorgesetzten informieren, dass die automatisierte Antwort durch den Systemadministrator erfolgen kann.
Auch für den Fall dass keine Vertretung besteht und /oder keine Weiterleitung der E-Mails erfolgt, muss in der automatisierten Antwort ein Hinweis darauf erfolgen.

(11) Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse des jeweiligen Beschäftigten nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Geschäftliche E-Mails werden zur Aufrechterhaltung des Geschäftsbetriebes an zuständige Beschäftigte weitergeleitet. Ist ein privater Charakter des Inhaltes dieser weitergeleiteten E-Mail ersichtlich, ist die E-Mail ohne weitere Kenntnisnahme des Inhaltes durch die jeweiligen Beschäftigten zu löschen. Eine Weiterleitung erfolgt nicht.

(12) Aus Wirtschaftlichkeits- oder IT-Sicherheitsgründen kann die Internetnutzung beschränkt werden. Dies kann beispielsweise folgendes beinhalten:

- Sperrung bestimmter Dienste der Internetnutzung
- Reduzierung auf bestimmte Internetanschlüsse
- Beschränkung des Massendatenverkehrs
- Beschränkung des Speicherplatzes

4. Verhaltensgrundsätze

(1) Die Beschäftigten haben jede Nutzung des Internets zu unterlassen, die geeignet ist, den Interessen der Einrichtungen oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Unternehmensnetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften /geltendes Recht verstößt. Dies gilt vor allem für

- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen
- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, blasphemischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen

- die Nutzung des Internets zur Erledigung privater Rechtsgeschäfte, insbesondere die Nutzung von Zahlungsfunktionen (Onlinebanking, Internethandel, eBay, etc.)
- die Nutzung von Onlineplattformen und Onlinespieleplattformen

Abrufen und Aufrufen heißt im Netz vorhandene Informationen mit IT-Systemen des Unternehmens zu zugreifen.

Verbreiten heißt einer Person oder einer Vielzahl von Personen oder einem unbestimmten Personenkreis über Internet-Dienste unter Verwendung von IT-Systemen des Unternehmens anzubieten.

Anbieten ist nur der Geschäftsführung bzw. nur mit deren Genehmigung gestattet.

(2) Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.

5. Verantwortlichkeit

Die Verantwortung für die Beachtung der vorgenannten Festlegungen und Hinweise obliegt der Geschäftsführung, sowie den Mitarbeitern. Diese haben insbesondere auch sicherzustellen, dass eine Nutzung des Internets durch Unbefugte vom Arbeitsplatz aus nicht erfolgt.

Hinweis:
Trotz des Einsatzes von Firewall oder Systemen und Software zum Schutz vor Schadsoftware ist das Ausspähen und Manipulieren von Daten durch Dritte nicht mit absoluter Sicherheit ausgeschlossen

6. Protokollierung und Kontrolle

(1) Alle eingehenden E-Mails werden durch eine Firewall, einen Spam-Filter sowie Virenscanner geprüft

(2) Die Verkehrsdaten für den Internetzugang werden mit Angaben von
- Datum und Uhrzeit
- Adressen von Absender und Empfänger (z.B. IP-Adressen)
- Benutzeridentifikation (z. B. Bei der Verwendung eines Proxy-Servers)
- der aufgerufenen Webseiten
- übertragene Datenmenge

protokolliert.
(3) die Protokolle nach Absatz (2) werden ausschließlich zu Zwecken der Analyse und Korrektur technischer Fehler
- Gewährleistung der Systemsicherheit
- Optimierung des IT-Netzes
- statistischen Feststellung des Gesamtnutzungsvolumens
- Stichprobenkontrollen gemäß Punkt 4
- Auswertungen gemäß Punkt 8 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

7. Maßnahmen bei Verstößen / Missbrauchsregelung

(1) Bei Verdacht auf missbräuchliche oder unerlaubte Nutzung des Internetzugangs (hervorgerufen beispielsweise durch ein erhöhtes Gesamtdatenvolumen oder auch die Kenntnisnahme nicht zulässiger im Internet angebotener Inhalte) gem. Nr. 3 und 4 dieser Vereinbarung durch einen Mitarbeiter findet unter Beteiligung des Datenschutzbeauftragten und bestellte IT-Fachkräfte eine Überprüfung des Datenverkehrs statt. Sind weitere Untersuchungsmaßnahmen (z. B. Offenlegung der IP-Adresse des benutzten Arbeitsplatzes oder weitere Überprüfungen) notwendig, werden diese, von den in Satz 1 genannten Personen veranlasst. Auf der Basis dieser Untersuchung wird ein Bericht erstellt, der dem Betroffenen ausgehändigt wird. Dieser ist anschließend dazu anzuhören.

(2) Ist aufgrund der stichprobenhaften, nicht-personenbezogenen Kontrollen bzw. der Auswertung der Übersicht des Datenvolumens eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung des Internetzugangs zu erkennen, so werden innerhalb von einer zu setzenden Frist von zwei Wochen nach der Anhörung die Stichproben weiterhin nicht-personenbezogen durchgeführt. Ergeben diese Stichproben bzw. die Auswertung der Übersicht des Datenvolumens keine Änderung im Nutzungsverhalten, so werden die Protokolle der folgenden zwei Wochen durch die in Absatz 1 genannten Personen stichprobenhaft personenbezogen ausgewertet. Hierbei wird wie im Falle des Verdachts einer missbräuchlichen Nutzung (Abs.1) vorgegangen. Zu den Verfahren nach Satz 1 und Satz 2 erfolgt eine entsprechende vorherige schriftliche Mitteilung an alle Beschäftigten, so dass deren Kenntnisnahme über die Maßnahmen gewährleistet werden kann.

(3) Ein Verstoß gegen diese Arbeitsanweisung kann neben den arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

8. Konzerninternes Netz

Zur Inventarführung der eingesetzten Hard- und Software sowie zur Netzwerkadministration und zur Benutzerunterstützung wird Software auf einem lokalen Server eingesetzt.

Aufzeichnungen und Auswertungen der System- oder systemnahen Software über Benutzeraktivitäten (Login /Logout, aufgerufene Programme, verbrauchte Systemressourcen, Zugang zu PC-Netzwerkservern usw.) dürfen ausschließlich zu den folgenden Zwecken benutzt werden:

Gewährleistung der Systemsicherheit

- Feststellung der Nutzungsdauer und -häufigkeit
- Analyse und Korrektur von technischen Fehlern im System
- Optimierung des Computersystems
- statistische Auswertungen ohne individuelle Kennung über den Zugriff auf Ressourcen im Netz

- Missbrauchskontrolle

Der Zugriff auf die entsprechenden Funktionen ist auf diejenigen Personen begrenzt, die für die Wartung der Hard- und Software sowie der Netzwerkadministration zuständig sind.

Die entsprechenden Dateien werden nur so lange gespeichert, wie dies zur Erfüllung der oben genannten Zwecke erforderlich ist.

Soweit mittels Software zur Unterstützung der Netzwerkverwaltung ein Zugriff auf die Arbeitsplatzrechner von Mitarbeitern /Mitarbeiterinnen möglich ist, so wird diese so installiert, dass nur die berechtigten Administratoren Zugriff auf die Endgeräte haben können.

Der Einsatz von Softwareprodukten mit Eskalationsmanagement (automatische Erzeugung von Alarm- und Aufmerksamkeitsmeldungen) bleibt auf technische Fehlermeldungen der Server- und Systemsoftware begrenzt. Darüber hinaus können die Mitarbeiter und Mitarbeiterinnen Software mit solchen Leistungsmerkmalen einsetzen, um sich selbst auf die Einhaltung von Fristen oder die Durchführung termingebundener Arbeiten aufmerksam machen.

9. Nutzung der Firmen IT

Alle Mitarbeiter verpflichten sich die Firmen-IT (u.a. Workstations, Notebooks, Server, Drucker usw.) schonend und sorgfältig zu nutzen. Die Nutzung der Firmen-IT darf nur zu betrieblichen Zwecken erfolgen.

Das Einbringen von Software auf Firmen-IT ist nicht zulässig. Die Nutzung privater Software auf Firmen-IT ist aus lizenzrechtlichen und sicherheitsbedingten Gründen untersagt.

Das Erstellen und Speichern privater Daten und Dokumente auf der Firmen-IT ist ebenfalls untersagt.

Die Nutzung privater Hardware (u.a. Speichersticks, PDAs, Notebooks, externe Festplatten, Mobiltelefone usw.) mit der Firmen-IT ist unzulässig.

10. Passwort-Gebrauch

Soweit technisch möglich, sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Die Geschäftsführung wird, soweit keine betrieblichen oder technischen Gründe entgegen stehen, jedem einzelnen berechtigten Nutzer einen Benutzernamen sowie ein Passwort zuweisen lassen.
Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen /Zeichen mit Sonderzeichen) zu gestalten.
Soweit technisch möglich ist jeder Mitarbeiter verpflichtet, sein Innitial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor- und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345)

Die Passwörter sind regelmäßig zu ändern und dürfen keinesfalls Dritten mitgeteilt oder schriftlich notiert werden.

11. Nutzung von mobilen Geräten (Smartphones, Tablets, Laptops etc.)

Soweit nicht ausdrücklich eine Zustimmung der Geschäftsführung erfolgt ist, darf die Nutzung von mobilen Geräten mit vom Unternehmen oder der IT freigegebenen Geräten ausschließlich für geschäftliche Zwecke erfolgen.
Häufig tritt Datenverlust durch Diebstahl eines Gerätes auf. Neben dem unmittelbaren Verlust des Gerätes kommt hinzu, dass die Daten, die sich auf dem Gerät befunden haben, durch Fremde eingesehen und missbraucht werden können. Um das Risiko eines (ungewollten) Datenverlustes zu verringern, sind nachfolgende Regeln zu beachten:

Nutzeridentifikation: Soweit technisch möglich sind Maßnahmen wie Kennwortschutz, PIN, Tastensperren, etc. zu verwenden.

- Weitergabe: Die Weitergabe an Dritte ist nicht zulässig.
- Verlust: Der Verlust eines Geräts ist unverzüglich der Geschäftsführung zu melden.
- Schnittstellen: Sämtliche Funk- (WLAN, Bluetooth etc.), Infratrot- und andere Kommunikationsschnittstellen sind zu deaktivieren, sofern diese nicht benutzt werden.
- Mobile Geräten dürfen nicht unbeaufsichtigt gelassen werden.
- Private mobile Geräte dürfen nicht an die IT Infrastruktur angeschlossen werden und es dürfen keine Server-Daten darauf gespeichert werden.

12. Regelung zur Speicherung von betrieblichen Daten und Dokumenten

Alle Mitarbeiter verpflichten sich alle Daten und Dokumente zentral auf dem Fileserver zu speichern. Nur so kann gewährleistet werden, dass alle Daten und Dokumente in den jeweils aktuellen Versionen gesichert werden können.
Das Abspeichern von Dokumenten und Daten auf der lokalen Festplatte ist untersagt. Von der Geschäftsführung beauftragte IT-Fachkräfte werden bei Bedarf die lokalen Festplatten prüfen und darauf gespeicherte Daten und Dokumente löschen, um einen reibungslosen Betrieb zu gewährleisten.

13. Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden dem Datenschutzbeauftragten mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken, Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können in einer ergänzenden Regelung vorgenommen werden.

Inkrafttreten

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft.

....

Datum Unterschrift Mitarbeiter(in)