IT-Benutzerrichtlinie für Mitarbeitende

Deutsches Rotes Kreuz Kreisverband Odenwaldkreis e.V.

Illigstraße 11

64711 Erbach

1. Einleitung

Diese IT-Benutzerrichtlinie regelt die Grundsätze für den Zugang und die Nutzung der Informationssysteme des Deutsches Rotes Kreuz Kreisverband Odenwaldkreis e.V. (nachfolgend „DRK“).

Ziel dieser IT-Benutzerrichtlinie ist die Herstellung der IT-Sicherheit, die Transparenz der Nutzungsbedingungen, die Transparenz der Maßnahmen zur Protokollierung und Kontrolle, die Sicherung der Persönlichkeitsrechte der Beschäftigten sowie die Unterstützung bei der nachhaltigen Umsetzung der getroffenen Maßnahmen zum Schutz von personenbezogenen Daten und der IT-Sicherheit.

Die Richtlinie dient als grundlegende Information für alle Mitarbeiter*innen im Hinblick auf den Umgang und Schutz personenbezogener Daten.

2. Geltungsbereich

Diese IT-Benutzerrichtlinie gilt für alle Beschäftigten und freiwillige Unterstützer*innen des DRK. Dazu gehören alle Beschäftigten, Unterstützenden, Auszubildenden, Praktikant*innen, Werkstudent*innen sowie Aushilfskräfte etc.. Externe Personen die regelmäßig für den DRK tätig sind, verpflichten sich nach dieser Richtlinie zu agieren.

Der DRK wird entsprechende Vorkehrungen treffen, damit diese Richtlinie auch für die externen Personen verbindlichen Charakter hat. Die Richtlinie gilt unabhängig vom Tätigkeitsort der Beschäftigten. Das heißt, dass die Richtlinie auch bei Tätigkeiten im Rahmen der „mobilen Arbeiten“ bzw. der Telearbeit im Home- oder Mobile-Office gültig ist.

3. Organisatorische Grundsätze

Die elektronischen Kommunikationssysteme und IT-Systeme stehen den Beschäftigten als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung. Die Absicherung des Zugangs zum Internet wird durch eine Firewall sichergestellt. Die Installation und Konfiguration von Web-Browsern, die IT-fachliche Betreuung der Beschäftigten sowie die Administration ihrer Internetberechtigungen erfolgt durch den IT-Support des DRK.

Sämtliche Computerarbeitsplätze müssen wirksam durch Virenschutzprogramme vor Schadsoftware gesichert werden. Diese Programme dürfen durch Beschäftigte nicht eigenständig manipuliert oder deaktiviert werden. Gleiches gilt für den Einsatz von Filterprogrammen, die den Zugriff auf Angebote mit rechtswidrigen oder strafbaren Inhalten sperren sowie für alle Sicherheitsprogramme und -einstellungen.

Der Erwerb von Geräten und Software folgenden Typs ist der Geschäftsleitung des DRK vorbehalten und muß vor einer eventuellen Anschaffung mit der Geschäftsleitung abgesprochen werden:

- Rechnersysteme (z.B. PC, „E-Book Reader“, Tablet-Rechner, mobile Rechner, Standrechner, Server)
- Telefone (GSM-, DECT-, Standtelefone), Telefon-Rechner-Einheiten („Smartphones“)
- Kameras, Videokameras, Projektoren
- Drucker, Etikettendrucker, Netzwerkgeräte, dazugehörige Peripherie und Verbrauchsmaterial (z.B. Druckerpatronen)
- Speicherkarten, USB Sticks, Festplatten, Switch, Router, Datenverbindungsgeräte (z.B. UMTS HSDPA, LTE Adapter)
- Software/Software-Lizenzen jeglichen Typs, Datendienste, Datentarife

Die Administration der Computer und Geräte der IT-Infrastruktur (z.B. das Hinzufügen oder Entfernen von Programmen und Konten, u.a. E-Mail, Social Media, Instant Messenger, Dateiaustausch, Einstellungen der Netzwerkkonfiguration, Änderungen der Verkabelung der Hardware), ist ausschließlich den zuständigen Administratoren erlaubt. Der Betrieb von IT Systemen jeglicher Art ist in den Netzen des DRK ist ausschließlich für Geräte des DRK erlaubt.

4. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen im DRK müssen Beschäftigte die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie sonstige diesbezügliche Regelungen des DRK berücksichtigen. Sollten Beschäftigte unsicher sein, ob und inwieweit Rechtsvorschriften oder sonstige Regelungen einzuhalten sind, sollten sie sich an ihren Vorgesetzten zur Klärung wenden. Eine Aufstellung wichtiger Rechtsgrundlagen entnehmen Sie Anlage 1 der IT Benutzerrichtlinie.

5. Schulung

Der DRK trägt Sorge dafür, dass die Beschäftigten die erforderlichen Schulungen und Anweisungen erhalten, die für den jeweiligen sicheren Umgang mit den IT-Systemen und Applikationen erforderlich sind.

6. Allgemeine Regelungen/Zulässigkeit der Nutzung

Die Nutzung der IT-Systeme und Applikationen im DRK ist ausschließlich zu dienstlichen Zwecken und im jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Jegliche private Nutzung ist untersagt.

Der Zugang zu den bereitgestellten Rechnersystemen und Konten wird nur Mitarbeiter*innen des DRK gewährt. Dritten (z.B. anwesenden Besuchern, betreuten Personen etc.) ist kein Zugang gestattet. Der Zugang zu Rechnersystemen und Konten muss z.B. durch ein Passwort vor allgemeinem Zugriff geschützt sein.

Jeder / jedem Nutzer steht ein eigenes Nutzerkonto in den IT Systemen der DRK zur Verfügung. Eine Weitergabe dieser Zugangsdaten an interne sowie externe Dritte ist nicht zulässig.

Über die dienstlichen E-Mail-Adressen eingehende private E-Mails werden wie private schriftliche Post behandelt, d.h. eingehende private Mails werden den betroffenen Beschäftigten zur alleinigen Kenntnis gegeben. Eingehende private E-Mails müssen von Beschäftigten nach Kenntnisnahme des privaten Charakters unverzüglich gelöscht werden. Die Beschäftigten müssen in solchen Fällen die Absender über die Regelung informieren, dass keine privaten Mails an die Mailadressen der Beschäftigten des DRK geschickt werden dürfen.

Wird bei den später benannten Kontrollmaßnahmen eine Zuwiderhandlung gegen diese Vorschrift festgestellt, werden diese Daten / private Mails ohne vorherige Einsichtnahme gelöscht.

Die Installation von Software zu privaten Zwecken ist untersagt. Im Übrigen darf nur lizenzierte Software auf IT-Systemen des DRK installiert werden, die seitens der Geschäftsleitung des DRK freigegeben worden ist. Jegliche Softwareinstallation muss im Vorfeld mit der Geschäftsleitung bzw. dem beauftragten IT Support des DRK abgestimmt werden bzw. muss durch diese autorisiert und durchgeführt werden. Dies betrifft auch den Testbetrieb von neuer Software.

Die Benutzung privater Software zu dienstlichen Zwecken ist nicht zulässig.

Die Benutzung privater Hardware zur Datenkommunikation darunter auch private Telefone und Smartphones zu dienstlichen Zwecken ist nur in begründeten Ausnahmefällen nach vorheriger schriftlicher Autorisierung durch die Geschäftsleitung zulässig. Ausgenommen davon ist die mündliche bzw. telefonische Kommunikation. Für die mündliche bzw. telefonische Kommunikation dürfen private Mobiltelefone und Smartphones verwendet werden. Private Smartphones sind während der Tätigkeit im DRK nur für eine Notfallerreichbarkeit zu nutzen. Das Aufzeichnen von Audio-, Video- und Bild-Daten mittels privater Geräte ist nicht gestattet. Hierfür dürfen ausschließlich Geräte des DRK verwendet werden.

Der Empfang, Versand sowie die Speicherung betrieblicher Mails auf privaten Smartphones oder Rechnersystemen ist nicht zulässig. Ausgenommen von dieser Regelung sind ausschließlich private Smartphones, die an das zentrale Mobile Device Management System des DRK Kreisverband Odenwaldkreis e.V. angebunden sind und deren Datenbereich somit zwischen privater und geschäftlicher Nutzung getrennt / unterteilt sind.

Die Nutzung privater Rechnersysteme im Rahmen des mobilen Arbeitens ist nicht zulässig.

Die Nutzung der AlDente App sowie eines Authenticators für die dienstliche 2-Faktor Authentifizierung ist zulässig.

7. Arbeitsplatz

Der Arbeitsplatz muss von den Beschäftigten so gestaltet werden, dass Besucher*innen oder sonstige Dritte keinen Zugang zu personenbezogenen Daten erhalten können, ohne hierfür berechtigt zu sein. Büros müssen nach dem Verlassen des Arbeitsplatzes grundsätzlich verschlossen werden.

Beim Verlassen des Arbeitsplatz-PCs müssen jeweilige Beschäftigte den PC „sperren“, sodass vor der erneuten Nutzung des IT-Systems und/oder der Applikationen eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr müssen die IT-Systeme insbesondere die Bildschirme so ausgerichtet werden, dass das Risiko der Kenntnisnahme durch Besucher oder Dritte ausgeschlossen wird.

Informationen in Papierform sollen so abgelegt werden, dass Besucher*innen oder sonstige Dritte keine Kenntnis von den Daten erhalten können. Vertrauliche Informationen müssen stets unter Verschluss gehalten werden.

Sollte die Umsetzung der zuvor benannten Vorgaben aufgrund räumlicher, baulicher oder die Ausstattung betreffender Gegebenheiten nicht möglich sein, haben die Beschäftigten dies bei der Geschäftsleitung schriftlich zu benennen.

8. Gebrauch von Passwörtern

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 IT-Abteilung wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, allen einzelnen berechtigten neuen Nutzer*innen einen Benutzernamen sowie ein Passwort zuweisen.

Passwörter müssen eine Mindestlänge von acht Zeichen haben. Das Passwort bitte alphanumerisch (Buchstaben, Zahlen, Sonderzeichen) gestalten.

Alle neuen Benutzer*innen sind verpflichtet, das Initial-Passwort unverzüglich zu ändern. Passwörter dürfen nicht offen einsehbar hinterlegt und niemals an Dritte weitergegeben werden. Wichtige administrative (nicht personenbezogene) Kennworte müssen verschlossen bei der Geschäftsleitung hinterlegt werden.

Passwörter müssen regelmäßig gewechselt werden. Die letzten fünf bereits genutzten Passwörter dürfen nicht wiederverwendet werden.

9. Schutz vor Schadinhalten

Zum Schutz vor Schadinhalten werden auf den IT-Systemen des DRK Virenschutzprogramme eingesetzt. Insbesondere eingehende E-Mail-Kommunikation wird durch die eingesetzten Virenschutzprogramme überprüft. Dabei kann es auch zur Löschung von E-Mails und Dateianhängen kommen. Für den Fall, dass Beschäftigte eine E-Mail mit – nach eigener Urteilsfähigkeit und nach eigenem Ermessen - einem unbekannten bzw. verdächtigen Dateianhang erhalten, haben sich diese unverzüglich an den IT Support zu wenden. Der unbekannte bzw. verdächtige Dateianhang darf erst nach Freigabe durch den IT-Support geöffnet werden. Bei der Nutzung von E-Mail als Kommunikationsmedium gilt "Sicherheit zuerst“- im Zweifelsfall sind verdächtige oder unbekannt Anhänge nicht zu öffnen. Ebenso sind – nach eigener Urteilsfähigkeit und nach eigenem Ermessen – verdächtige oder unbekannte Hyperlinks in Mails nicht zu öffnen.

10. Schutz vor unverlangter Werbung („Spam“)

Zum Schutz vor unverlangter Werbung per E-Mail wird auf dem Mailsystem des DRK ein sogenannter Spam-Filter eingesetzt. Der Einsatz des Spam-Filters erfolgt aus betrieblichen Gründen. Durch den Spam-Filter kann es dazu kommen, dass im Einzelfall E-Mails unterdrückt oder gelöscht werden.

11. Nutzung von E-Mail und Internet

Jegliche private Nutzung von E-Mail und Internet ist untersagt. Die Nutzung von E-Mail und Internet ist nur für dienstliche Zwecke erlaubt.

Dokumente, die personenbezogene oder andere sensible Daten enthalten, dürfen nicht unverschlüsselt im Internet oder via E-Mail übertragen werden. Eine Anleitung darüber, wie Dokumente vor dem E-Mail Versand verschlüsselt werden können, stellt der IT-Support bereit.

Das Abrufen und Ausführen von Dateien oder Programmen aus dem Internet ist nur von durch die Geschäftsleitung des DRK bekannt gegebenen Anbietern gestattet, soweit deren Inhalte für den dienstlichen Gebrauch benötigt werden. Dies betrifft auch „freie Software“ (Freeware) wie z.B. Bildschirmschoner, Tools, etc.

Urheberrechtlich geschützte Dateien, für die keine Lizenz und kein Nutzungsrecht vorhanden ist, dürfen nicht abgerufen und gespeichert werden.

Ermöglicht die Berechtigung der Beschäftigten das Abrufen und die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software, muss dies im Vorfeld des Abrufens bzw. der Installation von der Geschäftsleitung des DRK genehmigt werden.

Das Ausführen von aktiven Inhalten (z.B. Makros) in heruntergeladenen Dokumenten ist nur bei vertrauenswürdigen Anbietern gestattet. Im Zweifel muss dies vor der Ausführung von aktiven Inhalten mit dem IT Support des DRK abgestimmt werden.

Das Abrufen von für den DRK kostenpflichtigen Informationen oder Inhalten aus dem Internet muss bei der zuständigen Abteilungsleitung beantragt werden und bedarf der Genehmigung durch die jeweilige Abteilungsleitung.

Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen des DRK sogenannte Remote-Anwendungen bzw. Terminal-Emulationen sind grundsätzlich nicht zugelassen. Sollte dienstlicher Bedarf für Remote-Zugriffe bzw. Terminal-Emulationen bestehen, müssen diese bei der IT-Abteilung des DRK unter Angabe der Gründe beantragt werden.

Die Internet-Telefonie und Bildtelefonie sind – außer bei seitens der Geschäftsleitung zugelassenen Standard Anwendungen des DRK - grundsätzlich nicht zugelassen. Ausnahmen für den dienstlichen Gebrauch müssen ebenfalls beim IT-Support des DRK beantragt werden und sind nur mit der dafür zur Verfügung gestellten Software zulässig. Zur betrieblichen Nutzung zugelassene Standard Anwendungen für Internet- und Bildtelefonie sind – Stand Oktober 2024 – die Anwendungen Swyx (Server des DRK Kreisverbandes) für Telefonie und Videotelefonie sowie Microsoft Teams, Zoom, BigBlueButton, Jitsi sowie Cisco Webex.

Lesende Zugriffe auf das dienstliche E-Mail-Postfach durch jeweils benannte Vertreter*innen können während Abwesenheitszeiten wie Urlaub, Krankheit, etc. ohne gesonderte Abstimmung mit den Beschäftigten durch den IT-Support eingerichtet werden. Die Beschäftigten werden darüber informiert.

Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse der jeweiligen Beschäftigten nicht mehr zur weiteren Nutzung zur Verfügung. Die Beschäftigten sind angehalten, ihre außerbetrieblichen Kommunikationspartner*innen über diesen Umstand zu informieren. Dienstliche E-Mails werden zur Aufrechterhaltung des Dienstbetriebs an zuständige Beschäftigte weitergeleitet. Ist ein privater Charakter des Inhalts dieser weitergeleiteten E-Mail ersichtlich, muss die E-Mail ohne weitere Kenntnisnahme des Inhaltes durch die jeweiligen Beschäftigten gelöscht werden. Eine Weiterleitung erfolgt nicht.

Lesende Zugriffe auf das dienstliche E-Mail-Postfach durch jeweils benannte Vertreter*innen können mit Beendigung des Beschäftigungsverhältnisses ohne gesonderte Abstimmung mit den Beschäftigten, nach Freigabe durch die Geschäftsleitung, durch den IT-Support eingerichtet werden.

„Die zuvor beschriebenen lesenden Zugriffe auf das dienstliche E-Mail Postfach werden nur durchgeführt, wenn dies aus betrieblichen Gründen zwingend erforderlich ist. Sollten diese lesenden Zugriffe erfolgen, werden der Betriebsrat sowie der Datenschutzbeauftragte darüber informiert."

Den Beschäftigten ist während Ihrer Tätigkeit für den DRK keine Nutzung des Internets gestattet, die den Interessen des DRK und dessen Ansehen in der Öffentlichkeit schadet, die Sicherheit des Netzwerkes des DRK zu beeinträchtigt oder die gegen geltende Rechtsvorschriften bzw. die vorliegende Benutzerrichtlinie verstößt.

Zur Überprüfung der Einhaltung der Regelungen dieser Richtlinie werden ggf. zukünftig regelmäßige, nicht namensbezogene (nicht personenbezogene) Stichproben durchgeführt.

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

12. Protokollierung und Kontrolle

Alle eingehenden E-Mails werden durch einen Spam-Filter sowie einen Virenscanner geprüft.

Die Verkehrsdaten für den Internetzugang werden mit Angaben von

- Datum/Uhrzeit
- Adressen von Absender und Empfänger (z.B. IP-Adressen)
- den aufgerufenen Webseiten und
- übertragener Datenmenge

protokolliert.

Der Zugriff auf die Protokolldateien ist auf IT Support zur IT-fachlichen Bearbeitung und begrenzt.

Die bei der IT-fachlichen Bearbeitung der vorhandenen Protokolle einsehbaren personenbezogenen Daten, werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Richtlinie und den einschlägigen datenschutzrechtlichen Vorschriften.

Im Rahmen der Verfolgung von Straftaten, können die protokollierten Verkehrsdaten an Ermittlungsbehörden übergeben werden, insofern dafür eine rechtliche Verpflichtung besteht.

13. Nutzung von Messengern auf Endgeräten und Smartphones des DRK

Die Installation sowie die Nutzung von Messengern wie z.B. WhatsApp auf Endgeräten und Smartphones des DRK ist untersagt. Bereits bestehende Installationen solcher Software bzw. Apps müssen umgehend zu entfernt werden. Auf Endgeräten und Smartphones des DRK dürfen ausschließlich von der Geschäftsleitung freigegebene Messenger Software und Apps genutzt werden. Zum aktuellen Stand ist ausschließlich der Messenger „Signal" freigegeben.

14. Nutzung von Messenger Software auf privaten Endgeräten von Mitarbeiter*innen des DRK

Bei Installation sowie Nutzung von nicht freigegebenen Messenger Systemen wie z.B. „WhatsApp" auf privaten Endgeräten erlischt umgehend eine ggf. zuvor eingeräumte Autorisierung der Nutzungsberechtigung für dienstliche Nutzungszwecke des betroffenen privaten Endgerätes / Smartphones zur Datenkommunikation (z.B. Mail, etc.). Nicht von dieser Regelung betroffen ist die mündliche bzw. telefonische Kommunikation dienstliche Zwecke (siehe auch Punkt 6). Zum aktuellen Stand ist ausschließlich die Messenger App „Signal" für dienstliche Kommunikation via Messenger freigegeben. Ausgenommen von dieser Regelung sind ausschließlich private Smartphones, die an das zentrale Mobile Device Management System des DRK Kreisverband Odenwaldkreis e.V. angebunden sind und deren Datenbereich somit zwischen privater und geschäftlicher Nutzung getrennt / unterteilt sind.

15. Verhalten bei Sicherheitsvorfällen und Verlust von Geräten

Sollten Beschäftigte feststellen, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, müssen diese sich unverzüglich an die Geschäftsleitung und die Vorgesetzten wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht. Unter einem Sicherheitsvorfall ist unter anderem Folgendes zu verstehen:

- Verdacht auf unberechtigte Nutzung eines Rechnersystems
- Verdacht auf unberechtigten Zugang zu Büroräumlichkeiten
- Virenmeldung
- „Trojaner“
- Ungewöhnliches Fehlverhalten eines Rechnersystems (Störung)
- Verlust von Daten in digitaler oder analoger Form (CD, USB-Stick, Memory-Karte, Papier bzw. Ordner)
- Fehler, Schäden, Funktionsstörungen an IT-Geräten sowie der Verlust von IT-Geräten

16. Verantwortlichkeit

Die Verantwortung für die Beachtung der vorgenannten Festlegungen und Hinweise obliegt den zuständigen Stellen sowie den jeweiligen Beschäftigten. Diese müssen insbesondere auch sicherstellen, dass eine Nutzung des Internets durch Unbefugte vom Arbeitsplatz aus nicht erfolgt.

17. Weisungen

Die Beschäftigten sind verpflichtet hinsichtlich IT Sicherheit den Weisungen des IT-Support Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen des IT-Support bestehen, kann die Geschäftsführung eingebunden werden.

18. Nutzung mobiler Datenträger

Die Nutzung mobiler Datenträger (USB-Sticks, SD-Karten, DVDs etc.), die sich nicht im Eigentum des DRK befinden, ist nicht zulässig. Es dürfen keine mobilen Datenträger Dritter mit den Rechnersystemen des DRK verbunden werden.
Die Nutzung mobiler Datenträger ist generell auf das absolut notwendige Mindestmaß zu reduzieren.
Ab Q2/2024 ist die Nutzung mobiler Datenträger (auch DRK eigener Datenträger) nicht mehr zulässig.

19. Nutzung optischer Datenträger

Die Nutzung optischer Datenträger (CD, DVD, BD etc.), die sich nicht im Eigentum des DRK befinden, ist nicht zulässig. Es dürfen keine optischen Datenträger Dritter mit den entsprechenden Laufwerken der Rechnersysteme des DRK gelesen und/oder beschrieben werden.

20. Datenhaltung und Datenablage im Internet

Daten sind stets entsprechend der Vorgaben der Geschäftsleitung auf den vorgegebenen Speicherorten (unternehmenseigenes Mailsystem, Onedrive, Sharepoint Online, Teams, Serverlaufwerke) des DRK abzulegen

Das Speichern von Daten des DRK auf privaten Datenträgern, privaten Endgeräten oder externen, nicht genehmigten Plattformen bzw. Diensten, ist ausdrücklich untersagt.

Das Anfertigen privater Kopien geschäftlicher Daten (z.B. der Transport von Daten auf privaten USB- Datenträgern) ist nicht gestattet.

Die Ablage und Speicherung von Datenbeständen, Dokumenten, Dateien des DRK auf Speichersystemen im Internet (sogenannte File Sharing Systeme) ist nicht zulässig. Betroffen von dieser Vorgabe sind Systeme wie z.B. Dropbox etc.).

Eine Ablage oder Speicherung von Datenbeständen ist nur auf Internetspeichersysteme gestattet, die durch die Geschäftsleitung des DRK bekannt gegebenen wurden.

21. Geschützter/sicherer Druck auf öffentlich zugängliche Drucksysteme

Bei der Nutzung der Drucker und Multifunktionsgeräte im DRK muss bei Ausdrucken mit sensiblem bzw. personenbezogenem Inhalt immer auf die Einhaltung der Vertraulichkeit der Druckausgabe geachtet werden.

Druckvorgänge mit sensiblen bzw. personenbezogenen Inhalten dürfen nur beaufsichtigt auf Druckern erfolgen. Konkret bedeutet dies, dass Ausdrucke mit solchen Inhalten ungeschützt nur auf Drucker erfolgen dürfen, die sich in der unmittelbaren Umgebung des Anwenders befinden.

Werden sensible bzw. personenbezogene Inhalte auf einem Drucker gedruckt, der sich nicht in unmittelbarer Umgebung des Anwenders befindet, muss die Funktion des sicheren Drucks aktiviert werden, sodass der Ausdruck erst nach Eingabe einer PIN am Ausgabegerät erfolgt insofern dieser für den jeweiligen Drucker verfügbar ist.

22. Erstellung von Kopien vorhandener Softwareprodukte

Die Erstellung von Kopien der durch den DRK erworbenen oder selbst erstellten Softwareprodukten ist nur durch explizit benannte Personen zulässig. Die Lizenzbedingungen der Softwarehersteller müssen eingehalten werden.

23. Auslagerung von Datenbeständen und Mobiles Arbeiten

Personenbezogene und unternehmensinterne Daten dürfen nur durch autorisierte Mitarbeiter*innen mit Genehmigung und nach Unterzeichnung der Datenschutzverpflichtung für die Durchführung von mobilem Arbeiten außerhalb des Geländes des DRK verbracht werden. Dies betrifft sämtliche Transportwege wie z.B. in analoger Form, per Datenträger, per Mail, per Internetportal etc.

24. Vertraulichkeit und Geheimhaltung

Der Zugriff auf Datenbestände des DRK ist erst nach Unterzeichnung der „Verpflichtung auf die Vertraulichkeit“ und im jeweiligen Rahmen der betrieblichen Aufgabenerfüllung zulässig.

Die Mitarbeiter*innen sichern zu, dass alle im Rahmen der betrieblichen Aufgabenerfüllung bzw. des Vertragsverhältnisses bekannt gewordenen personenbezogenen Daten und sonstigen Informationen streng vertraulich behandelt und geheim halten werden.

Die Mitarbeiter*innen sichern ebenso zu, nur auf Datenbestände des DRK zuzugreifen, die für die betriebliche Aufgabenerfüllung erforderlich sind.

25. Nachhaltigkeit bei der IT-Nutzung

Mitarbeiter*innen sind angehalten nachhaltig, d.h. sparsam und schonend mit den informationstechnischen Ressourcen umzugehen. Ausdrucke sollten nur dann angefertigt werden, wenn dies erforderlich ist. Rechnersysteme, Notebooks, Bildschirme und Drucker müssen zu Arbeitsende ausgeschaltet werden. Mit Speicherplatz auf den Serversystemen und Arbeitsplätzen muss sparsam umgegangen werden. Nicht mehr benötigte Daten sind zu löschen, insofern keine Verarbeitungsgrundlage sowie keine Aufbewahrungspflicht.

26. Sichere Vernichtung analoger und digitaler Datenbestände

Digitale und analoge personenbezogene Datenbestände dürfen nicht ohne eine sichere und fachgerechte Vernichtung entsorgt werden. Es ist nicht zulässig, bestehende digitale Datenspeicher oder analog vorliegende Dokumente mit personenbezogenen Inhalten über den Hausmüll zu entsorgen. Datenspeicher dieser Art (z.B. USB Sticks, Festplatten, sonstige Datenlaufwerke) müssen fachgerecht vernichtet und entsorgt werden.
Bestehende analoge Dokumente mit personenbezogenen Inhalten dürfen ebenso nicht über den Hausmüll/Papiermüll entsorgt werden. Dokumente dieser Art müssen mit einem geeigneten Schredder der Sicherheitsstufe P4 gem. DIN Norm 63399 (oder besser) vernichtet oder über einen vergleichbar sicheren Dienstleister entsorgt werden.

27. Datenschutzbeauftragter

Das DRK hat einen Datenschutzbeauftragten bestellt, der den Mitarbeitenden wie auch den Leitungskräften als Ansprechpartner für Fragen des Datenschutzes und der IT-Sicherheit zur Verfügung steht. Der Datenschutzbeauftragte ist unter der Mailadresse datenschutz@drk-odenwaldkreis.de erreichbar. Der Datenschutzbeauftragte ist auf die Vertraulichkeit bei eventuellen Anfragen durch Beschäftigte – auch im Innerverhältnis des DRK – verpflichtet.

_____

Erbach im Oktober 2024
Frank Sauer, Vorstand des DRK KV Odenwaldkreis e.V.

Erklärung zur IT-Benutzerrichtlinie des Deutsches Rotes Kreuz Kreisverband Odenwaldkreis e.V.

Hiermit erkläre ich, dass ich die „IT-Benutzerrichtlinie des Deutsches Rotes Kreuz Kreisverband Odenwaldkreis e.V.“ zur Kenntnis genommen habe und mich den Vorgaben entsprechend verhalte.

_____ _____

Ort, Datum Name, Unterschrift

Anhang 1
Wichtige Rechtsgrundlagen bei der Nutzung von Informationssystemen und betrieblicher Aktivitäten im Internet
Version 1.0, Stand: August 2024

Datenschutzgrundverordnung – DSGVO:
Link: https://www.dsgvo-gesetz.de

Bundesdatenschutzgesetz:
Link: https://www.dsgvo-gesetz.de/bdsg/

Hessisches Datenschutz und Informationsfreiheitsgesetz
Link: https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHEV1IVZ

Sozialgesetzbuch SGB X - §67 bis § 85a
Link: https://www.sozialgesetzbuch-sgb.de/sgbx/67.html

Urheberrechtsgesetz:
Link: https://www.gesetze-im-internet.de/urhg/

Telemediengesetz:
Link: https://www.gesetze-im-internet.de/tmg/

Telekommunikationsgesetz:
Link: https://www.gesetze-im-internet.de/tkg_2021