**Richtlinie zur Daten- und IT-Sicherheit**

**für Mitarbeitende der DRK-Gliederungen**

1. **Einleitung**

In fast jeder DRK-Gliederung werden Daten vorwiegend elektronisch verarbeitet. Die verarbeiteten Daten reichen von Stammdaten bis hin zu besonders schützenswerten Daten. Viele Gliederungen sind darüber hinaus mit Daten konfrontiert, die keinesfalls in Hände Dritter fallen dürfen – sei es aus Gründen des Datenschutzes oder weil es sich um vertrauliche Verbandsdaten handelt.

Daten-Sicherheit im Allgemeinen und speziell IT-Sicherheit sind daher unverzichtbar für jede DRK-Gliederung. Verbandsdaten müssen bestmöglich geschützt werden. Dies gilt sowohl für den Versuch, diese Daten auszuspionieren, als auch für die Gefahr des Datenverlustes durch technische Gebrechen.

1. **Sicherer Umgang mit personenbezogenen Daten**

Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

Besondere schützenswerte Daten umfassen Informationen u.a. über die politische, religiöse und philosophische Überzeugungen, *Gesundheit* und Gewerkschaftszugehörigkeit.

Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung, d. h. jeder darf selbst entscheiden was mit seinen Daten passieren soll. Das Speichern und Verarbeiten von personenbezogenen Daten sind nur unter Zustimmung des Betroffenen zulässig.

*Bitte folgende Punkte beachten:*

* Personenbezogene Daten müssen geheim gehalten werden. Nur bei schriftlicher Zustimmung dürfen diese Daten an Dritte weitergegeben werden.
* Bei Weitergabe der Daten muss auf einen sicheren Kommunikationsweg geachtet werden. Ein unverschlüsseltes E-Mail erfüllt diese Anforderung NICHT.
* Nach dem Ausscheiden aus dem DRK dürfen personenbezogene Daten, die den Mitarbeitenden zugänglich gemacht wurden, nicht weitergeben oder für andere Zwecke nutzen.

1. **Clear Desk Policy**

Unter der Clear Desk Policy versteht man, dass Mitarbeitende alle vertraulichen Dokumente, die sich am Arbeitsplatz befinden, verschließen. Unberechtigte Personen (Reinigungspersonal, unbefugte andere Mitglieder, oder Besucher) dürfen keinen Zugriff darauf erhalten.

*Bitte folgende Punkte beachten:*

* Bei Verlassen des Arbeitsplatzes müssen alle Ausdrucke, Kopien oder dergleichen so verstaut werden, dass diese Dokumente und mobile Datenträger nicht für Dritte zugänglich sind.
* Keine Ausdrucke im Drucker/Kopierer liegen lassen
* Passwortnotizen nicht am Arbeitsplatz aufbewahren.
* Beim Verlassen des Arbeitsplatzes Bildschirmschoner aktivieren. (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes   
  Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.

1. **Passwörter**

Ein Passwort ist wie einen Schlüssel zur Wohnung oder zum Haus. Zuhause möchte man auch ein gutes Schloss besitzen, welches vor einem unbefugten Zutritt schützt. Genauso verhalten sich auch Passwörter. Passwörter schützen vor unbefugten Zutritt.

*Bitte folgende Punkte beachten:*

* Nie das gleiche Passwort für unterschiedliche Zugänge verwenden. Eine Passwortdatenbank evtl. verwenden (z.B. www.keepass.info). Kennwörter, die mindestens 12 Zeichen haben verwenden. Ein Passwort muss aus einem Großbuchstaben, Kleinbuchstaben, Ziffer und einem Sonderzeichen bestehen, um halbwegs sicher zu sein.
* Niemals Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, etc. verwenden. Diese werden bei Angriffen zuerst ausprobiert.
* Keine Begriffe aus einem Wörterbuch verwenden (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden. Auch Eigennamen, geografische Begriffe etc. dürfen nicht verwendet werden.
* Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.) sind ebenfalls ungeeignet. Sie können von Anderen leicht beim Beobachten der Passworteingabe erkannt werden.
* Passwörter niemals weitergeben! Auch andere Mitglieder oder die IT-Betreuung benötigen dieses Kennwort nicht.
* Einen Satz mit den Anfangsbuchstaben für das Passwort verwenden. Z. B.
* Die Arbeit beginnt jeden Tag um 7 Uhr - DAbjTu7U
* Am Samstag arbeite ich von 9 bis 13 Uhr - ASaiv9-13U
* am 26.10. ist Nationalfeiertag - a26.10.=N
* Jeder ist für seine Kennwörter verantwortlich! Bei Verdacht, dass ein Dritter das Kennwort kennt, das Passwort unverzüglich ändern.

1. **Dokumente und Datenträger richtig entsorgen**

Sorglos weggeworfene Dokumente stellen ein ernstes Sicherheitsproblem dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Dokumente, Datenträger (USB Stick, Festplatte, SD Karte, CD/DVD…) sicher entsorgt werden. Für die sichere Entsorgung eignet sich ein Dokumenten-Schredder oder ein Dienstleistungsunternehmen, welches sich auf die sichere Entsorgung spezialisiert hat. Das Dienstleistungsunternehmen stellt nach der Entsorgung ein Zertifikat aus, welches die fachgerechte Entsorgung bestätigt.

*Bitte folgende Punkte beachten:*

* Datenträger oder wichtige Dokumente auf keinen Fall in den Papierkorb werfen! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen, müssen die Datenträger und Dokumente sicher entsorgt werden.
* Nicht mehr benötigten Datenträger dem Verantwortlichen übergeben (IT-Verantwortliche) bzw. einer eigens zu diesem Zweck bestimmten Person, die für die sichere Entsorgung zuständig ist.

1. **Umgang mit mobilen IT-Geräten**

Mobile IT Geräte (Notebooks, Smartphones...) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar. Portable Geräte sind für Diebe ein attraktives Ziel.

*Bitte folgende Punkte beachten:*

* Das Gerät nicht unbeaufsichtigt lassen
* Das Gerät nicht anderen Personen überlassen
* Bei Passworteingabe am Gerät auf Sichtschutz achten – ähnlich wie bei einem Bankomaten.
* Privaten Cloud-Speicher nicht für Verbandsdaten nutzen
* Nur Anwendungen installieren, die als vertrauenswürdig und sicher bekannt sind und von frei gegeben wurden.
* Einen Diebstahl oder Verlust sofort dem Verantwortlichen melden

1. **Internetnutzung**

Auch beim normalen Surfen im Internet lauern Gefahren, die nicht gleich als solche erkannt werden. Es liegt in der eigenen Verantwortung, solche Bedrohungen zu erkennen und entsprechend darauf zu reagieren.

*Bitte folgende Punkte beachten:*

* *Gesunden Menschverstand nutzen!* Wenn sie z.B. keinen Handy Vertrag mit T-Mobile haben, handelt es sich bei eingegangen E-Mails von T-Mobile meistens um betrügerische E-Mails.
* Keine persönlichen Daten übermitteln, vor allem nicht, wenn die Verbindung nicht als sicher (HTTPS im Browser) markiert wird.
* Websites, die mit dem Download kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken, ist grundsätzlich zu misstrauen.
* Das Herunterladen von Dateien kann, abgesehen von der Gefahr des Einschleppens von Schadsoftware, auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Vereinsrechner gespeichert ist.
* Meiden von Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in gecrackter Form, zum Download angeboten wird.
* Keine Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten aufrufen. Das kann gravierende rechtliche Probleme, auch für das DRK, nach sich ziehen.
* Bei Unsicherheiten immer fragen!

1. **E-Mail Nutzung**

E-Mail gehört schon fast zur Standardausrüstung eines Arbeitsplatzes. Dadurch lohnt es sich auch für Kriminelle diese Form der Kommunikation zu nutzen. Somit landen aber auch unerwünschte Mails mit Schadprogrammen verseuchte Nachrichten in den Posteingang. Solche unerwünschten Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen ca. zwei Drittel des weltweiten E-Mail-Aufkommens aus.

*Bitte folgende Punkte beachten:*

* Keine E-Mails öffnen, wenn der Absender oder Betreffzeile verdächtig erscheinen.
* Niemals Dateianhänge öffnen, die verdächtig sind. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Werden die beigelegten Dateien erwartet und passen sie zum Absender, oder kommen sie völlig unerwartet?
* Keine E-Mails mit Spaßprogrammen öffnen, da diese Schadsoftware enthalten können.
* Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen auf keinen Fall weitergeben.
* Oftmals kann in einem E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Vorsichtig sein: In betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als im Mail zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren“ in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.
* Keine Spam-Mails beantworten! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch das Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
* Auch andere Mitarbeitende über verdächtige Zusendungen informieren. Die aktuellen E-Mails, die als Phishing-Versuche oder Virus-Mails erkannt wurden besprechen, um gemeinsam die typischen Kennzeichen kennenzulernen. Man kann auf diese Weise sehr rasch die Erkennungsfähigkeit trainieren und verbessern.
* Auch hier gilt, bei Unklarheiten und Unsicherheiten die Verantwortliche Person fragen!
* Bei Urlaubsantritt oder bei Abwesenheit an den Abwesenheitsassistenten denken, um die Absender über ihre Abwesenheit zu informieren.
* Bei der Versendung von E-Mails ist grundsätzlich darauf zu achten, wenn mehrere Personen außerhalb der Gliederung mit einer E-Mail angeschrieben werden, dass die E-Mail-Adressen im Feld BCC. eingefügt werden (sofern keine Einwilligungen der Personen vorliegt).

1. **Social Engineering**

Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt. Social Engineers geben sich gerne als Mitarbeiterinnen oder Mitarbeiter aus. Vielleicht behaupten sie auch, eine Behörde oder zu vertreten. Ihre Opfer werden durch verbandsinternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege“ an Ihre Hilfsbereitschaft oder drohen in sonstiger Form. Kommt ein Social Engineer bei einer Mitarbeiterin oder einem Mitarbeiter nicht ans Ziel, wird der Angriff bei der nächsten Ansprechperson wiederholt – bis er erfolgreich ist.

*Bitte folgende Punkte beachten:*

* Bei Telefonanrufen oder E-Mails skeptisch sein, speziell wenn der Wunsch oder der Auftrag außergewöhnlich ist.
* Die Angelegenheit mit dem Verantwortlichen vorher besprechen.
* Achtung: dass Social Engineering sehr oft angewandt wird, aber meistens lange Zeit unentdeckt bleibt.
* Keine vertraulichen Informationen per Telefon oder E-Mail weitergeben.

1. **Private Nutzung der IT**

Die Nutzung der IT für private Zwecke sollte vermieden werden. Dies betrifft sowohl die Nutzung der Geräte an sich (PC, Laptop, Smartphone…) als auch das verbandsinterne E-Mail-Postfach (E-Mail) und den Firmeninternetanschluss. Sollte die private Nutzung von ihrer Seite notwendig sein, holen sie sich bitte eine Ausnahmegenehmigung.

1. **Warnungen und Fehlermeldungen**

Warnungen oder Fehlermeldungen, die nicht selbst verursacht wurden, bzw. die nicht gelöst werden können, müssen unverzüglich dem Verantwortlichen gemeldet werden.

1. **Wechselmedien**

Als Wechselmedien gelten alle externen Datenträger wie z.B. USB-Sticks, SD Karten, externe Festplatten, CDs, DVDs, Smartphones, die per USB angeschlossen werden. Der Einsatz stellt ein großes Sicherheitsrisiko dar. Speziell wenn diese Datenträger aus externer Quelle stammen. Auf diesen Wechselmedien kann sich Schadsoftware verstecken, welche das gesamte Netzwerk lahmlegen kann. Generell ist die Verwendung von Wechselmedien untersagt. Ausnahmen mit dem Verantwortlichen abklären.

1. **Installation von Applikationen (Anwendung, Software)**

Die Installation von Applikationen auf geschäftliche IT-Geräte ist untersagt. Dies gilt sowohl für Windows Geräte (PCs, Notebooks, Server), aber auch für verbandseigene Mobilgeräte wie Smartphone und Tablets. Falls eine Applikation benötigt wird, die verantwortliche Person ansprechen. Auch harmlos wirkende Applikationen können Schadsoftware enthalten oder sind lizenzrechtlich nicht für den Verbandseinsatz freigeben.

1. **Drucker und Faxgerät**

Um Irrläufer zu vermeiden ist beim Fax darauf zu achten, dass die richtige Zielnummer eingegeben wird (am besten im Fax die Nummer hinterlegen). Zudem sollte darauf geachtet werden, dass der richtige Empfänger auch das Fax erhält, d. h. es sollte vor dem versenden des Faxes der Empfänger davon unterrichtet werden, wann das Fax versendet wird, so dass dieser dann vor Ort sein kann. Grundsätzlich sollte aber vorab geprüft werden, ob die Versendung mit dem Faxgerät überhaupt notwendig ist.

Bei Druckaufträgen sollte der Drucker mit einer Druckabruf PIN ausgestattet sein, so dass der Berechtigte über die Eingabe einer PIN den Druckvorgang am Drucker aktivieren kann. Ist dieser Abruf an Drucker nicht möglich, dann sollte die Person, welche den Druckvorgang auslöst, sich zeitnah am Drucker befinden, um unberechtigte Dritte keinen Zugang zu den Daten zu ermöglichen.

1. **Nutzung von Messenger-Diensten**

Die Nutzung von WhatsApp ist zwar nach wie vor sehr verbreitet, steht jedoch seit Jahren wegen Datenschutzmängeln und intransparenter Verarbeitung von Nutzerdaten in der Kritik.

Die Problematik bei WhatsApp ist primär die Synchronisation der Kontakte auf dem Smartphone. Wenn bei der Einrichtung der App dem zugestimmt wird, erhält WhatsApp Zugriff auf alle Kontakte, welche sich auf dem Smartphone befinden, ohne dass die Betroffenen vorher eingewilligt haben. Die Einwilligung ist aber nach der DS-GVO Voraussetzung, damit die Datenweitergabe rechtskonform ist. Zudem werden die Daten unverschlüsselt an WhatsApp versendet, so dass evtl. weitere unberechtigte Dritte Zugriff auf die Kontaktdaten bekommen könnten.

*Bitte folgende Punkte beachten:*

* Es wird empfohlen einen datenschutzkonformen Messenger-Dienst in der gesamten DRK-Gliederung zu verwenden (z.B. Threema, Signal).
* Beim Einrichten von WhatsApp darf die Synchronisation der Kontakte durch WhatsApp nicht zugelassen werden. Dann ist es zwar nicht mehr möglich, die App aktiv zu nutzen, da keine Nachrichten mehr per WhatsApp versendet werden können, aber es kann dem anderen Kommunikationsteilnehmer die Telefonnummer auf anderem Wege zur Verfügung gestellt werden. Sobald man darauf eine Nachricht auf von einem Kontakt erhält, kann nun davon ausgegangen werden, dass die Einwilligung des Kommunikationsteilnehmers vorliegt. Eine rechtskonforme Kommunikation über WhatsApp ist nun durch die Einwilligung möglich.