Weisung des Direktors für den Gebrauch von Informatikinstrumenten und die Benützung von elektronischen Kommunikationseinrichtungen

Inhaltsverzeichnis

1 Einführung: Zweck und Aufbau der Weisung

Die vorliegende Weisung bezweckt die Regelung der Nutzung von Informatik- und Netzwerkeinrichtungen des Schweizerischen Roten Kreuzes (SRK). Die Weisung liefert Klarheit bezüglich den Rechten und Pflichten der Mitarbeitenden[1] und ASP-Kunden im Umgang mit den zur Verfügung stehenden Informatikinstrumenten und elektronischen Kommunikationseinrichtungen (E-Mail, Internet).

Die Mitarbeitenden sollen durch einen vernünftigen Umgang mit Technik und Daten ihren Teil zur Sicherheit des Netzwerks und zur Geheimhaltung vertraulicher, geschäftlicher Daten beitragen.

Die Weisung ist in 5 Bereiche aufgeteilt:

- **Allgemeines**, insb. Grundsatz, Regelung des persönlichen Geltungsbereichs und der Verbindlichkeit, Begriffsdefinitionen, Verantwortlichkeiten, Benutzerunterstützung und Ausbildung (Kapitel 2)
- **Informatikinstrumente und Sicherheit im SRK-Netzwerk**, insb. die Beschaffung und der Einsatz von privaten Informatikinstrumenten, Vorgaben für das An- und Abmelden am Informatiksystem, Umgang mit Passwörtern/Sicherheitstoken und der Einsatz von Virenschutzprogrammen (Kapitel 3)
- **Daten und Geheimhaltung**, insb. Datenhoheit, Umgang mit besonders schützenswerten Daten, Geheimhaltungsverpflichtung für Mitarbeitende und externe Dienstleister (Kapitel 4)
- **Nutzung von elektronischen Kommunikationseinrichtungen** (E-Mail und Internet), insb. die private Nutzung, Überwachung und Sanktionen sowie die generelle Speicherung von E-Mails in einem E-Mailarchiv (Kapitel 5)
- **Umgang mit Smartphones und Tablets**, insb. Sicherheitsmassnahmen zum Schutz der auf Smartphones vorhandenen Daten (Kapitel 6)

Mit der vorliegenden Weisung macht das SRK von seinem Weisungsrecht nach Art. 321 OR Gebrauch. Weitere Informationen zu Arbeitsrecht und Datenschutz, insb. die Reglementierung des privaten Gebrauchs von elektronischen Kommunikationseinrichtungen, stehen auf der Website des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (http://www.edoeb.admin.ch/) zur Verfügung.

2 Allgemeines

2.1 Grundsatz

Die Benutzung von Informatik- und Netzwerkeinrichtungen muss in direktem Zusammenhang mit den Tätigkeiten des Arbeitgebers stehen und soll dazu dienen, die unternehmerischen Ziele werkzeuggestützt und effizient zu erreichen.

2.2 Geltungsbereich und Verbindlichkeit

2.2.1 Allgemeiner personeller Geltungsbereich

Der Geltungsbereich dieser Weisung umfasst:

- alle Mitarbeitenden der Geschäftsstelle SRK

[1] Alle Formen gelten jeweils sinngemäss für beide Geschlechter.

- Praktikanten, Temporär- und Aushilfspersonal
- Freiwillige der Geschäftsstelle SRK
- externe Dienstleister, die über SRK-Benutzerkonten verfügen müssen (z.B. Berater, Informatiker, Projektleiter, Supervisoren)

Die Weisung wird an alle betroffenen Personen versandt. Neue Mitarbeitende der GS SRK erhalten sie bei ihrer Einführung vom Personalwesen ausgehändigt.

2.2.2 ASP-Kunden

Für Kunden der ICT Services, welche die Informatik-Dienstleistungen im Auftragsverhältnis (Application Service Providing ASP) nutzen, ist diese Weisung ebenfalls verbindlich. Sofern es zwischen Mitarbeitenden der Geschäftsstelle SRK und den ASP-Kunden Unterschiede oder abweichende Regelungen gibt, werden diese hierin explizit erwähnt.

2.2.3 Verbindlichkeit

Diese Weisung ist für alle betroffenen Personen verbindlich. Sie räumt den Mitarbeitenden Rechte und Pflichten ein, deren Nichtbeachtung sanktioniert werden kann.

2.3 Begriffsdefinitionen

Begriff	Definition
Apps	Aus dem Englischen für „Application“, bezeichnet grundsätzlich jede Form von Anwendungsprogrammen. Heute wird die Bezeichnung allerdings fast ausschliesslich für Programme verwendet, die für Smartphones und Tablets programmiert sind und über einen Online-Shop bezogen und werden können.
ASP	Application Service Providing, Software-Nutzung über Terminal Server.
ASP-Kunden	Kunden der ICT Services, welche die Informatik-Dienstleistungen im Auftragsverhältnis nutzen
Backup	Sicherung der Datenbestände auf ein Speichermedium (Harddisk, Magnetband etc.)
Bluetooth	Technologie, die die Datenübertragung zwischen zwei Geräten auf kurze Distanz ermöglicht.
Cloud Service	Services im Internet wie z. B. iCloud, Dropbox, Picasa, SkyDrive. Diese Services sind teilweise kostenlos oder zu einer geringen Gebühr benutzbar. Sie werden u. a. verwendet, um Daten auf Internet-Speichern abzulegen.
Elektronische Kommunikationseinrichtungen	Internet, E-Mail, Fax und Telefon
GS	Geschäftsstelle SRK
https	Verschlüsselte Übertragung von Websites und Daten im Internet
ICT	Information Communication Technology
Informatikinstrumente	umfassen die Informationssysteme und die Informationstechnik, im engeren Sinne Hard- und Software inkl. Netzwerktechnik
Informationssysteme (IS)	sind Anwendungen (Software-Programme) zur computergestützten Bearbeitung und Führung der Aufgaben. Die Informationssysteme bestehen aus den zur Ausführung der Geschäftsfunktionen notwendigen Daten, den dazu benötigten Verarbei-

	tungsfunktionen und den zugehörigen organisatorischen Regelungen und Vereinbarungen.
Informationstechnik (IT)	ermöglicht die Realisierung und den Betrieb der computergestützten Informationssysteme. Sie gliedert sich in Maschinen (Server, PC, Drucker, Scanner, Digitalkameras, etc), Netzwerke, Programme und die für deren Einsatz notwendigen technischen Verfahren
Schlüssel	Kennwort oder Anweisung, anhand derer ein Text ver- und entschlüsselt werden kann. (⇨*Verschlüsselung*)
Service	Dienst oder Dienstleister
Single Point of Contact	zentrale Anlaufstelle, über welche alle Meldungen, Anfragen, Aufträge und Probleme zu ICT Services weiter geleitet werden.
Smartphone	Ein Mobiltelefon (vormals „Natel“), das ausser der reinen Telefonie-Funktionen zusätzliche Computer-Funktionalitäten zur Verfügung stellt, meistens zum Surfen im Internet und Daten synchronisieren, aber auch mit vielen zusätzlich installierbaren Programmen (⇨ *Apps*).
Tablet	Ein Laptop-ähnliches Gerät, das über Berührungen mit dem Finger oder einem speziellen Stift bedient werden kann. Als bekannter Vertreter dieser Art sei das iPad von Apple genannt.
Verschlüsselung	Verfahren, mit dem ein Text mithilfe eines bestimmten ⇨Schlüssels in eine unleserliche Zeichenfolge verwandelt wird, die nur mithilfe des Schlüssels wieder entschlüsselt werden kann.

2.4 Verantwortlichkeit

Die Verantwortlichkeit betreffend Kontrollen zur Einhaltung der nachfolgenden Regelungen obliegt den Linienvorgesetzten. Vorbehalten bleibt die Regelung in Ziff. 5.3.

2.5 Benutzerunterstützung

2.5.1 Power User und Informatik-Koordinator

Die Mitarbeitenden wenden sich bei Fragen und Problemen in erster Linie an ihren zugewiesenen Power User. Dieser steht ihnen bei Anwenderproblemen unterstützend zur Verfügung. Im Bedarfsfall kontaktiert er das Service Desk der ICT Services.

Bei ASP-Kunden kann der Informatik-Koordinator die Rolle des Power Users einnehmen.

2.5.2 Service Desk ICT Services

Das **SERVICE DESK** ist der **SINGLE POINT OF CONTACT** für alle User bzw. Power User. Sämtliche Anfragen, Meldungen, Bestellungen und dergleichen sind ausschliesslich an das Service Desk zu richten. Bei grösseren Problemen und bei Abwesenheiten der Power User steht den Benutzern das Service Desk der ICT Services telefonisch und per E-Mail zur Verfügung.

Mail: servicedesk@redcross.ch

Telefon: 031 / 387 72 60

Falls der Power User bzw. Informatik-Koordinator anwesend ist, sind die Anfragen und Meldungen an ihn zu richten.

Die Mitarbeitenden werden vom Service Desk informiert, wenn Ausfälle auftreten oder ausserordentliche Wartungsarbeiten anstehen.

2.5.3 Meldepflicht der Mitarbeitenden

Störungen, Fehler und Vorfälle, welche die Vertraulichkeit, Integrität, Verfügbarkeit oder Sicherheit der Informatikinstrumente beeinträchtigen oder gefährden könnten, sind den ICT Services unverzüglich mitzuteilen.

2.6 Ausbildung der Mitarbeitenden

2.6.1 Schulung im SRK

Damit die Mitarbeitenden die umfangreichen Möglichkeiten, welche die Informatikinstrumente ihnen bieten, auch effizient und optimal nutzen können, müssen sie über entsprechendes Wissen und die nötigen Ausbildungsmöglichkeiten verfügen. Das SRK bietet allen Mitarbeitenden und den ASP-Kunden im Schulungsraum an der Taubenstrasse 8 in Bern die Möglichkeit, sich in Kursen weiterzubilden. Die Zuständigkeit für das interne Bildungswesen (Kursangebot, Beratung, Durchführung) liegt bei der Abteilung Personal der Geschäftsstelle. Anfragen sind zu richten an: personalentwicklung@redcross.ch

2.6.2 Neue Mitarbeitende

Neue Mitarbeitende der Geschäftsstelle SRK erhalten anlässlich ihrer Einführung durch die ICT Services ein Merkblatt, in dem sie auf die Besonderheiten der SRK-Informatikinstrumente hingewiesen werden. Bei den ASP-Kunden obliegt diese Einführung den Informatik-Koordinatoren.

3 Informatikinstrumente und Sicherheit im SRK-Netzwerk

3.1 Informatikinstrumente im SRK-Netzwerk

3.1.1 Beschaffung

GS SRK

Die Beschaffung von Informatikinstrumenten erfolgt zentral durch die ICT Services. Beschaffung durch den Mitarbeitenden ist nicht gestattet. Die Informatikinstrumente verbleiben im Besitz des SRK.

ASP-Kunden

Die Beschaffung von Informatikinstrumenten (Hardware oder Software auf lokalen PCs) ist Sache der Kunden. Auf Anfrage und gegen Verrechnung können die ASP-Kunden die Dienste der ICT Services bei der Beschaffung in Anspruch nehmen. Bei der lokal installierten Software sind die Kunden für die Lizenzen selbst verantwortlich. Alle Geräte verbleiben im Besitz des Kunden. Die Kunden sind verantwortlich, die Garantieanforderungen einzuhalten. Bei Interventionen der ICT Services sind ihnen allfällige Garantien mitzuteilen.

3.1.2 Hardware

Darunter fallen alle Arbeitsplatz-PCs, Notebooks mit oder ohne Dockingstationen, Bildschirme, Arbeitsplatzdrucker und andere Peripheriegeräte. Für die Benutzung ist der jeweilige Mitarbeitende verantwortlich. Er kann sein Gerät mit entsprechender Nutzungsweisung einer Drittperson für einen temporären Einsatz an Ort und Stelle überlassen.

Datei- und Datenbankserver, Netzwerkkommunikationsgeräte und Netzwerk- und Sicherheitseinrichtungen dürfen nur von Mitarbeitenden der ICT Services oder von bezeichneten Dritten (externe Berater und Fachkräfte) bedient werden.

Eine private Vermietung der Firmengeräte durch den Mitarbeitenden ist nicht gestattet.

Installationen

Sowohl Hardware- wie auch Software-Installationen werden, sofern nicht anders vereinbart, durch Mitarbeitende der ICT Services vorgenommen. Dies gilt auch im Falle von Bürowechseln.

Ohne Rücksprache mit ICT Services ist das Installieren von peripheren Geräten wie z.B. Drucker, Scanner, Modems untersagt.

Das Installieren und Benutzen von Fremdsoftware ist aus lizenzrechtlichen und sicherheitstechnischen Gründen untersagt.

Pflege / Reinigung der Hardware

Die Pflege und Reinigung ist Sache des Mitarbeitenden. Geeignetes Reinigungsmaterial ist bei den Büromaterial-Ausgabestellen oder bei den Power Usern resp. Informatik-Koordinatoren erhältlich.

3.1.3 Software

Es gelangen nur Programme zum Einsatz, die von den ICT Services getestet und freigegeben wurden und für welche das SRK bzw. der ASP-Kunde die entsprechenden Lizenzen erworben hat.

3.1.4 Zusätzlich benötigte Informatikinstrumente

Zusätzlich benötigte Informatikinstrumente sind den ICT Services schriftlich mit speziellem Formular anzumelden. Das entsprechende Formular ist beim Service Desk verfügbar.

3.2 Private Informatikinstrumente

3.2.1 Verwendung im SRK-Netzwerk

Private Informatikinstrumente wie Scanner, Notebooks etc. dürfen grundsätzlich nicht im Firmennetz eingesetzt werden. Ausnahmen werden durch die ICT Services bewilligt. Es besteht kein Anspruch auf finanzielle Vergütung oder Entschädigung. Die Versicherung solcher Geräte ist Sache des Eigentümers.

3.2.2 Kauf von privaten Informatikinstrumenten

Beschaffung

Grundsätzlich wird jedem Mitarbeitenden eine (1) Arbeitsplatz-Infrastruktur kostenlos zur Verfügung gestellt. Private Informatikinstrumente für den Einsatz zuhause oder mobile ICT-Ausrüstungen für unterwegs müssen vom Mitarbeitenden selbst beschafft und finanziert werden, auch wenn diese nebst der privaten Verwendung auch für die Arbeitserfüllung im Auftrag des Arbeitgebers verwendet werden. Spezialfälle werden gesondert geregelt und von der Linie resp. dem Direktor bewilligt. Sofern die Lizenzbestimmungen des Softwareherstellers Kopien für den Heimgebrauch (sog. Right for home use) zulassen, kann ein Antrag gem. Ziff. 3.1.4 gestellt werden. Die Versicherung dieser Geräte oder Garantieverlängerung obliegen dem Mitarbeitenden. Das SRK entrichtet hierfür keine finanzielle Unterstützung.

Unterstützung durch die ICT Services

Für Produkteberatung, Einkaufsberatung, Kauf, Installationen, Reparaturen oder Betreuung für privates Material gewähren die ICT Services keine Unterstützung. Davon ausgenommen sind PDAs gemäss dem „Merkblatt Einsatz und Finanzierung mobile Kommunikationsmittel für die Geschäftsstelle und das Sekretariat der Kantonalverbände SRK“ sowie Antiviren-Programme gemäss der Ziffer 3.6.2.

3.2.3 Verwendung privater Informatikinstrumente für den Zugriff auf Programme und Daten des SRK (Terminalserverzugriff über Internet)

Der Mitarbeitende muss sicherstellen, dass sein privates Informatikinstrument ausreichend geschützt ist. Der Mitarbeitende stellt dies folgendermassen sicher:

1. Regelmässiges (monatliches) Aktualisieren des Betriebssystems
2. Aktualisieren des Virenschutz-Programms nach Aufforderung, siehe auch Ziff. 3.6.2
3. Aktualisieren der Virenschutz-Signaturen (mind. täglich oder kürzere Zeitabstände)
4. Periodisches Überprüfen der Festplatten mit Virenschutzprogramm (monatlich)
5. Aktivierung der Windows-Firewall (ab Windows XP). Wenn nicht möglich, Installation eines Firewall-Programms und dieses aktuell unterhalten (z.B. Avira Premium Security Suite)

Es besteht die Möglichkeit, mit Microsoft Windows-fremden Informatikinstrumenten auf die Terminalserver des SRK zuzugreifen, z.B. mit Apple, Linux oder Android. Die vorgenannten Bestimmungen zum Schutz solcher Geräte gelten für diese ebenfalls.

Die Einhaltung und Durchführung oben genannter Bestimmungen obliegt dem Mitarbeitenden und müssen von diesem oder in dessen Auftrag von einer Drittperson ausgeführt werden. Die Arbeitgeber richten hierfür weder finanzielle Entschädigung aus, noch kann hierfür Arbeitszeit abgerechnet werden.

3.3 Erreichbarkeit der Server in der GS von ausserhalb

Für alle Mitarbeitenden der SRK Terminal Services besteht die Möglichkeit, die Server in der Geschäftstelle SRK via Internet zu erreichen. Der Zugang erfolgt stets mit der üblichen zugewiesenen Benutzer-Authentisierung über das Zugangsportal www.redcrosswork.ch.

3.4 An- und Abmelden am Informatik-System

3.4.1 Benutzerauthentisierung

Die Anmeldung am System des SRK erfolgt über eine benutzerspezifische Authentisierung. Über diese Authentisierung werden die Zugriffsberechtigungen auf die einzelnen Bereiche des Netzwerks sowie der Programme geregelt. Die Verantwortung für die dem Mitarbeitenden zugewiesenen Authentisierungsmittel trägt jeder Mitarbeitende selbst. Die Authentisierungsmittel sind persönlich, nicht übertragbar und dürfen Dritten in keiner Weise zugänglich gemacht werden. Missbrauch hat eine sofortige Meldung an den Linienvorgesetzten zur Folge.

3.4.2 Abmeldung vom System

Wird der Arbeitsplatz für mehr als 10 Minuten verlassen, muss die Arbeitsstation vor unberechtigtem Zugriff gesichert werden (--> Lock Workstation). Die Terminal-Server sperren die Sitzungen nach 10-minütiger Inaktivität automatisch. Die Arbeitsplatz-PCs inkl. Bildschirme und lokale Arbeitsplatzdrucker müssen bei Abwesenheit, vor allem über Nacht und am Wochenende, abgeschaltet werden.

3.5 Passwort / Logincode

3.5.1 Vertraulichkeit

Passwörter sind persönlich, nicht übertragbar und absolut vertraulich zu behandeln. Sie dürfen weder sichtbar notiert noch für Dritte in irgendeiner Weise zugänglich sein.

3.5.2 Passwortwechsel

Ein Passwortwechsel wird vom System alle 12 Monate verlangt. Während 5 Passwortwechseln kann dasselbe Passwort nicht erneut verwendet werden.

3.5.3 Kreieren von Benutzerpasswörtern

Passwörter dürfen nie in unmittelbarem Zusammenhang mit dem Mitarbeitenden stehen (z.B. der Name des Kindes oder Partners, das Geburtsdatum, Telefon-, AHV-, Auto-Nummer). Ausserdem ist davon abzuraten, existierende Worte als Passwort oder Teil davon zu benutzen. Grundsätzlich gilt, je komplexer ein Passwort ist, desto sicherer ist es. Wie sicher ein Passwort ist, kann unter www.datenschutz.ch überprüft werden.

Eine hilfreiche Methode zum Kreieren sicherer und trotzdem merkbarer Passwörter ist, sich einen treffenden Satz auszudenken und jeweils die Anfangsbuchstaben und Satzzeichen als Passwort zu verwenden. Also zum Beispiel: „**I**ch **u**nd **m**ein **H**und **h**aben **e**ine **E**-Mail **A**dresse**!**“ ergibt das Passwort **IumHh1EA!**

3.5.4 Passwort-Auflagen

Das Passwort muss mindestens 6 Zeichen lang sein und mindestens **drei der folgenden vier** Auflagen erfüllen:

- mindestens 1 Grossbuchstabe A, B, C, …
- mindestens 1 Kleinbuchstabe a, b, c, …
- mindestens 1 Ziff. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
- mindestens 1 Sonderzeichen .,:;-_!?=+“*ç%&/() …

(Beachten Sie, dass Sonderzeichen bei anderen Sprachen nicht auf denselben Tasten angeordnet sind wie auf deutschsprachigen Tastaturen).

Passwörter dürfen ausserdem nicht aus dem Benutzerkürzel oder Teilen davon bestehen.
Diese Passwort-Auflagen können jederzeit verschärft werden.

3.5.5 Passwort-Sperre

Aus Sicherheitsgründen wird das Benutzer-Konto nach dreimaliger Fehleingabe des Passworts automatisch gesperrt. Das Entsperren des Kontos wird durch das Service Desk vorgenommen.

3.5.6 Logincode

Jeder Benutzer muss beim Login neben Benutzernamen und Passwort noch einen nur kurze Zeit gültigen Logincode eingeben. Dieser Logincode wird vom System auf eine hinterlegte Adresse geschickt. Dies kann entweder eine Mobiltelefon-Nummer oder eine E-Mail Adresse sein.

Die Benutzer sind verantwortlich dafür, diesen Logincode an keine Drittpersonen weiterzugeben. Erhält der Benutzer den Logincode auf sein privates Mobiltelefon, hat er keinen Anspruch auf Entschädigung seitens des SRK (ausgenommen davon ist der fakultative Lohnanteil beim Hinterlegen der Mobiltelefon-Nummer gemäss Blatt Lohnnebenleistungen).

ICT Services garantiert die zweckgebundene Nutzung der hinterlegten Mobiltelefon-Nummern. Die Nummern werden weder intern noch extern irgendwelchen anderen Stellen weitergegeben.

3.6 Virenschutz

3.6.1 PC-Arbeitsstationen

Auf den Terminal-Servern der ICT Services sind alle Mitarbeitenden durch den Virenschutz des SRK geschützt. Die im Netzwerk des SRK gespeicherten Dokumente werden laufend geprüft. Des Weiteren befindet sich auf jeder PC-Arbeitsstation ein lokales Virenschutzprogramm, welches automatisch und periodisch mit den neusten Virensignaturen versorgt wird.

Die ICT Services sind verantwortlich für aktuelle Virenüberwachungsprogramme auf den Arbeitsplatzsystemen SRK und bei den ASP Kunden. Grundsätzlich werden alle PCs kontinuierlich auf Viren geprüft. Das Virenschutzprogramm darf nie ausgeschaltet werden.

3.6.2 Laptop, mobile Geräte, PC zuhause

Mobile Geräte, welche sporadisch ins SRK-Netzwerk angeschlossen werden oder via Internet auf die Terminalserver zugreifen, müssen zwingend mit einem Virenschutzprogramm mit aktualisierten Virensignaturen versehen sein.

Für Beratung zu geeigneten Virenschutzprogrammen steht der Service Desk zur Verfügung.

3.7 Zugang zu Maschinenräumen und Netzwerkverteilern

Zugang zu Maschinenräumen und Netzwerkverteilern haben:

- alle Mitarbeitenden der ICT Services
- der Hausdienst
- Feuerwehr
- vom Leiter ICT Services oder dessen Stellvertretung bezeichnete Personen (z.B. Berater und externe Fachkräfte)

Die Bezeichneten verfügen über die entsprechenden Zugangsschlüssel und sind für das korrekte Schliessen der Türen verantwortlich. Drittpersonen, Mitarbeitende der GS und ASP-Kunden dürfen diese Zonen nur in Begleitung eines Mitarbeitenden der ICT Services betreten.

4 Daten und Geheimhaltung

4.1 Datenhoheit

Die Datenhoheit obliegt immer dem Mitarbeitenden. Dies bedeutet, dass der Mitarbeitende für die Qualität seiner Daten die volle Verantwortung trägt.

4.2 Datenschutz

Die auf dem Netzwerkserver gespeicherten Daten sind vor unberechtigtem Zugriff geschützt. Jeder Mitarbeitende hat nur Zugriff auf die für ihn notwendigen Ablagebereiche (Verzeichnisse). Geschäftsdaten dürfen aus Sicherheitsgründen nie auf der lokalen Harddisk des Arbeitsplatz-PCs gespeichert werden.

4.3 Umgang mit besonders schützenswerten Daten und Persönlichkeitsprofilen

Besonders schützenswerte Personendaten und Persönlichkeitsprofile geniessen gemäss Datenschutzgesetz (DSG) den höchsten Schutzbedarf.

Zu den besonders schützenswerte Personendaten zählen gemäss Art. 3 DSG Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen. Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Das SRK verfügt über viele solcher Daten, z.B. Patientendaten (Ambulatorium Folter- und Kriegsopfer, HIV-Diagnosen), Daten über Mitarbeiter etc.

Daher gilt für das Handling von besonders schützenswerten Daten und Persönlichkeitsprofilen:

- Daten nur via Terminalserver-Infrastruktur bearbeiten
- Daten per Mail nur innerhalb der redcross.ch-Domäne zu versenden (ASP-Kunden innerhalb eigener Mail-Domäne, z.B. srk-bern.ch)
- nicht gebrauchte Ausdrucke dieser Daten (auch Entwürfe) immer mit Aktenvernichter (Shredder) vernichten.

Nicht erlaubt ist:

- Daten via E-Mail unverschlüsselt übers Internet zu versenden (nicht nach Hause zum Weiterbearbeiten)
- Daten auf austauschbaren Wechselmedien (Diskette, CD-ROM, DVD, USB-Stick etc.) unverschlüsselt zwischen zu speichern
- Daten auf Notebooks mit unverschlüsselten Harddisks zwischen zu speichern und zu bearbeiten
- den Arbeitsplatz ohne vorheriges Blockieren der Arbeitsstation (CTRL+F2) für mehr als 10 Minuten zu verlassen
- die Zwischenablage der unverschlüsselten Daten im von allen Benutzern einsehbaren Transferverzeichnis T: auf dem Dateiserver
- Papierausdrucke unvernichtet und in lesbarer Form in den Papierkorb zu werfen (→Papier-Shredder).

4.4 Datensicherheit

Sämtliche auf den Datei- und Datenbankservern abgespeicherten Daten inkl. aller Datenbank- und DMS-Daten werden durch die ICT Services jede Nacht gesichert und sind extern ausgelagert.

4.5 Geheimhaltung und Meldung

4.5.1 Vertraulichkeit, berufliche Schweigepflicht, Geschäftsgeheimnisse

Alle nicht frei der Öffentlichkeit zugänglichen Daten des Arbeitgebers sind als vertraulich zu behandeln und gegenüber Dritten geheim zu halten. Geschäftliche Daten dürfen nicht an Drittpersonen weitergegeben werden, solange dies nicht in direktem Zusammenhang mit geschäftlichen Belangen steht, und ohne dass die ausdrückliche Erlaubnis des Verfassers der Daten vorliegt.

Die Verletzung der beruflichen Schweigepflicht kann strafrechtlich verfolgt werden (mit Haft oder Busse bestraft werden kann, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat (Art. 35 DSG)). Im Unterschied zur in Art. 321 StGB geregelten Verletzung des Berufsgeheimnisses braucht es zur Verletzung des Datengeheimnisses keine bestimmte Berufszugehörigkeit. Auch die Verlet-

zung der vertraglichen oder gesetzlichen Pflicht, Geschäftgeheimnisse geheim zu halten, ist gemäss Art. 162 StGB strafbar.

4.5.2 Geheimhaltungsverpflichtung des externen Dienstleisters

Der externe Dienstleister erlangt durch Unterstützungs- und Beratungsarbeiten Einsicht in Daten des SRK und der ASP-Kunden. Alle einsehbaren Daten und Geschäftsverbindungen sind als vertraulich zu behandeln und gegenüber Dritten geheim zu halten. Die eingesehenen Daten dürfen auf keine Art und Weise abweichend von den notwendigen Arbeiten (Beratung, Wartung, Einrichtung etc.) verwendet werden.

Die Verletzung der Geheimhaltungspflicht hat zivil- und strafrechtliche Folgen (Art. 162 StGB, Verletzung des Fabrikations- und Geschäftsgeheimnisses).

Der Dienstleister unterzeichnet im Rahmen des jeweiligen Auftrags eine bindende Geheimhaltungserklärung.

4.5.3 Meldung

Falls der Mitarbeitende irrtümlicherweise vertrauliche Daten einsehen kann, die nicht für ihn bestimmt sind, hat er dies seinem Linienvorgesetzten zu melden. Der Mitarbeitende stellt sicher, dass nicht weitere unberechtigte Mitarbeitende in die vertraulichen Daten einsehen können.

5 Nutzung von elektronischen Kommunikationseinrichtungen

5.1 E-Mail

5.1.1 Rechtliche Relevanz der E-Mail-Kommunikation

Dem Mitarbeitenden ist bewusst, dass E-Mails rechtlich relevant sind:

- Bestellungen, Vereinbarungen und per E-Mail geäusserte Willenserklärungen sind in den meisten Fällen rechtsverbindlich. Eine handschriftliche Unterschrift benötigen nur die wenigsten Geschäftsabschlüsse.
- Gemäss Geschäftsbücherverordnung ist man verpflichtet, alle geschäftsrelevanten E-Mails während 10 Jahren aufzubewahren.
- Durch E-Mailkommunikation können strafrechtlich und zivilrechtlich relevante Taten begangen werden (Spam, Mobbing, Viren, Ehrverletzungen, Verletzung des Daten- und Berufsgeheimnisses etc.)

5.1.2 Nutzungsbestimmung

Das elektronische Mail-System des SRK dient dem geschäftlichen Informations- und Datenaustausch mit internen und externen Geschäftspartnern. Die angemessene, private Benutzung ist unter den Voraussetzungen von Ziff. 5.1.3 und 5.1.4 erlaubt.

5.1.3 Private Benutzung

Die massvolle, gelegentliche Nutzung zu privaten Zwecken während der Arbeitszeit ist erlaubt, sofern dadurch die Arbeitsleistung und die technischen Ressourcen der ICT Services nicht beeinträchtigt werden.

Sämtliche ein- und ausgehenden Mails der Geschäftsstelle und von ASP-Kunden (sofern der Service „Mailarchivierung“ abonniert wurde) werden laufend automatisch archiviert und während mindestens 10 Jahren aufbewahrt. Dies gilt nicht nur für geschäftliche, sondern auch für private Mails. Wer dies aus Gründen des Persönlichkeitsschutzes nicht will, muss für seine privaten Mails eine externe Webmailadresse benutzen (gmx, hotmail, gmail, etc.).

Private E-Mails sind im Betreff als solches zu kennzeichnen (Betreff: Privat). Die Einsicht des Arbeitsgebers in private E-Mails richtet sich nach Ziff. 5.1.9 sowie Ziff. 5.1.10.

5.1.4 Generell nicht erlaubt sind

- das Versenden und Weiterleiten von Mail-Beilagen wie z.B. ausführbare Programme (Dateierweiterungen .exe, .vbs und andere), Spiele, Kettenbriefe etc.;
- das Verwenden der geschäftlichen E-Mail-Adresse zur Registrierung für private Dienstleistungen (z. B.: Privates eBay-Konto);
- das Versenden von E-Mails mit gefälschten Absenderadressen;
- das Versenden von Massen-Mails (Spamming, Art. 3 lit. o Bundesgesetz gegen den unlauteren Wettbewerb - UWG);
- das Antworten auf Spam- oder Phishing-Mails (als Spam- oder Phishing-Mail erkennbare E-Mails sind ungeöffnet zu löschen);
- die Belästigung anderer Personen und Mobbing per E-Mail;
- das Versenden und Weiterleiten von Comics, Fun-Videos und dergleichen, aus Gründen des Virenschutzes und der Eindämmung der Datenmenge;
- das Versenden und Weiterleiten von unsittlichen und strafrechtlich relevanten Inhalten
- das Versenden von Geschäftsgeheimnissen an Unberechtigte; die Zustellung von vertraulichen Daten an berechtigte Personen hat verschlüsselt zu erfolgen;
- das Versenden von privaten E-Mails, die grösser als 3 MB sind.

5.1.5 Maximale Grösse von E-Mails inkl. Anhänge

Die Grösse der E-Mails inklusive allfälliger Anhänge ist auf 25 MB beschränkt. Andere Firmen und Provider haben meist weit niedrigere Beschränkungen, daher sollte ein E-Mail im externen geschäftlichen Verkehr höchstens 3 bis 5 MB aufweisen. Grosse Dateien können über Komprimierungsprogramme wie z.B. WinZip komprimiert werden. Falls die Anhänge nicht auf die gewünschte Grösse reduziert werden können, sollte das E-Mail auf mehrere Sendungen aufgeteilt werden.

5.1.6 E-Mail und Sicherheit

Verschlüsselung von E-Mails

Beim Versand von (unverschlüsselten) E-Mails bleiben mehrere Sicherheitsanforderungen unerfüllt. Es fehlt an der Vertraulichkeit der Nachricht, d.h. sie kann potenziell von Dritten eingesehen werden. Die Integrität der Nachricht ist nicht sichergestellt, d.h. unbefugte Dritte können die Nachricht abfangen und verändern. Die Authentizität des Absenders ist nicht garantiert, d.h. die Nachricht stammt unter Umständen nicht vom angegebenen Absender. Die Verschlüsselung stellt zumindest die Vertraulichkeit und Integrität der Nachricht sicher.

Vertrauliche Daten sollten vor deren Versand mit der Verschlüsselungssoftware auf dem Terminal Server resp. im Programm Outlook verschlüsselt werden. Der Power User oder Informatik-Koordinator ist dem Informatik-Anwender hierbei behilflich.

Der Entscheid, ob die zu versendenden Daten zu verschlüsseln sind, richtet sich nach der Weisung des Direktors betreffend den Informationsschutz im SRK. Alternativ kann für vertrauliche Nachrichten auch die Briefpost oder Fax eingesetzt werden.

Welche Daten nur verschlüsselt per E-Mail verschickt werden dürfen, ist in Ziff. 4.3 geregelt.

5.1.7 E-Mail Postfach eintretender Mitarbeitender

Postfächer und Kalender von neu eintretenden Mitarbeitenden werden vor Stellenantritt der neuen Person nur auf deren explizite Einverständniserklärung hin für Linienvorgesetzte oder

Stellvertreter freigegeben. Die neuen Mitarbeitenden sind dabei selbst verantwortlich dafür, solche Freigaben nach Stellenantritt wieder entfernen zu lassen.

5.1.8 E-Mail-Postfach austretender Mitarbeitender

Der Mitarbeitende muss alle privaten Elemente aus seinem Postfach löschen bzw. auf einen persönlichen Datenträger, den er mitnehmen kann, abspeichern. Die geschäftlichen E-Mails, die weiterhin benötigt werden oder noch in Bearbeitung sind, hat er an seinen Stellvertreter, zuständigen Vorgesetzten oder Nachfolger weiterzuleiten oder entsprechend abzulegen. Nach dem letzten Arbeitstag des betreffenden Mitarbeitenden wird sein E-Mail-Postfach von ICT Services gesperrt.

5.1.9 Einsicht des Arbeitgebers und des Stellvertreters in E-Mails

Die Vorgesetzten können auf Verlangen hin mit ICT Services, **nach expliziter Einverständniserklärung der betroffenen Mitarbeitenden**, geschäftliche E-Mails einsehen. Die Einsichtnahme dient einerseits der Leistungs- und Geschäftskontrolle, andererseits um bei Abwesenheiten des Mitarbeitenden auf geschäftsrelevante E-Mails zugreifen zu können.

Der Arbeitgeber darf den Inhalt von **privaten E-Mails**, solange diese als solche erkennbar sind, nicht einsehen (Pflicht, die Persönlichkeit des Mitarbeitenden zu achten; Art. 328 und 328b OR). Vorbehalten bleibt das Einsichtsrecht nach Einholung des Einverständnisses gemäss Ziff. 5.1.10.

5.1.10 Beweissicherung, Einsicht bei begründetem Verdacht

Falls konkrete Anhaltspunkte auf Verletzung des Strafgesetzbuchs unter Verwendung von E-Mails bestehen (z.B. ein begründeter Verdacht auf Verletzung des Berufs- und Datengeheimnisses, Art. 320 StGB und Art. 35 DSG), hat das SRK das Recht, entsprechendes Beweismaterial zu sichern.

Für die Beweisaufnahme, insbesondere für das Öffnen privater E-Mails, werden die entsprechenden staatlichen Untersuchungsbehörden beigezogen.

Der Direktor kann die privaten E-Mails des Mitarbeitenden einsehen, falls dies zwingend notwendig ist, um den Verdacht besser zu begründen oder zu zerstreuen. Dazu wird jedoch die vorgängige schriftliche Einwilligung des Arbeitnehmers für das Öffnen der privaten E-Mails benötigt.

5.1.11 Sanktionen

Der Direktor kann bei Missbrauch der geschäftlichen E-Mail bzw. bei Verstoss gegen die Bestimmungen in Ziff. 5.1 Sanktionen gemäss Ziff. 5.3.5 ergreifen.

5.2 Internet

5.2.1 Nutzungsbestimmung

Das Internet dient der geschäftlichen Informationsbeschaffung für den Mitarbeitenden. Die massvolle, gelegentliche Nutzung zu privaten Zwecken während der Arbeitszeit ist erlaubt, sofern dadurch die Arbeitsleistung sowie die technischen Ressourcen der ICT Services nicht beeinträchtigt werden und die folgenden Regeln beachtet werden.

Im Internet ist eine riesige Fülle von Informationen frei verfügbar, was dazu verleiten kann, diese ohne Prüfung der Qualität zu nutzen. Das Urteil über Nützlichkeit und Qualität der online gefundenen Informationen bleibt dem Mitarbeitenden überlassen.

5.2.2 Generell nicht erlaubt sind:

- das Herunterladen und Installieren von Browser Plug-Ins und (Gratis-)Programmen
- die Verwendung von Online-Spielen
- das Erstellen oder Verbreiten von schädlichen Programmcodes (z.B. Viren, Trojaner, Würmer)
- Ausspionieren von Passwörter
- der Zugriff auf rassistische, pornographische, extremistische oder andere widerrechtliche und unsittliche Inhalte
- Hacking, namentlich:
    - unbefugtes Eindringen bzw. versuchtes Eindringen in fremde Computersysteme
    - treffen von Vorkehrungen zur Störung des Betriebs von Computern oder Netzwerken (z.B. Distributed Denial of Service Attacks)
    - unautorisiertes Absuchen von internen und externen Netzwerken und Computern auf Schwachstellen (z.B. Port-Scanning)
- sofern dies nicht in geschäftlichem Auftrag erfolgt:
    - die Teilnahme an Börsenforen und das Online-Handeln (z.B. Aktien, Fonds, Wertpapiere, Güter) und E-Banking
    - das Verschieben von Dateien über das FTP-Protokoll (File Transfer Protocol)
    - die Teilnahme an Online Auktionen und Versteigerungen (z.B. ebay, Ricardo), sofern nicht im Interesse des Arbeitgebers gehandelt wird
    - die Benutzung von Internet-Radiostationen oder Internet-Fernsehen, sofern die Nachrichtenbeschaffung nicht im Interesse des Arbeitgebers erfolgt.

Die Aufzählung ist nicht abschliessend.

5.2.3 Teilnahme in Newsgroups, Blogs und Social Networks

Die Teilnahme an Newsgroups (Diskussionsforen), Blogs (Internet-Tagebücher) oder Social Networks (Xing, Facebook, Twitter, LinkedIn, Partyguide usw.), die nicht in direktem Zusammenhang mit der beruflichen Tätigkeit stehen, ist nicht erlaubt. Bei Meinungsäusserungen ist die Neutralität der Rotkreuzbewegung, insbesondere des SRK (bei ASP-Kunden = deren Institution) zu respektieren. Für Mitarbeitende unserer ASP-Kunden gilt Vorgenanntes gleichermassen.

5.2.4 Multimedia-Stationen

Müssen für geschäftliche Zwecke Dokumente oder Bilder gescannt, Datenträger beschrieben oder Internet-TV oder –Radio benutzt werden, stehen den Mitarbeitenden an allen Standorten der Geschäftsstelle Multimedia-Stationen zur Verfügung. Die Power User sind über die korrekte Handhabung informiert und leisten den Mitarbeitenden im Bedarfsfalle Hilfestellung.

5.3 Aufzeichnungen, Kontrolle und Massnahmen gegen Missbrauch

5.3.1 Aufzeichnung des Internet-Surfverhaltens

Aus Sicherheitsgründen wird sämtlicher Internetverkehr laufend von den Firewall-Servern des SRK aufgezeichnet und protokolliert. Aufgezeichnet wird, wer von woher wie viel Informationen bezogen hat resp. wer wohin wie viel Informationen gesendet hat. Der effektive Informationsinhalt, der übermittelt wurde, wird nicht aufgezeichnet.

Die Protokollierungen werden nach einer gewissen Zeit gelöscht. Im Rahmen von Sanktionsverfahren oder Strafverfolgungen werden die Protokollierungen bis zur Beendigung der Verfahren aufbewahrt.

Heruntergeladene Webseiten verbleiben im Zwischenspeicher des Browsers oder des SRK-internen Proxy-Servers[2]. Die Inhalte sämtlicher Zwischenspeicher werden nach einer gewissen Zeit automatisch gelöscht.

5.3.2 Aufzeichnung des E-Mail-Verkehrs

Sämtliche ein- und ausgehenden Mails der Geschäftsstelle und von ASP-Kunden (sofern der Service „Mailarchivierung“ abonniert wurde) werden unabhängig vom Inhalt (d.h. auch E-Mails mit privatem Inhalt) laufend automatisch archiviert und während mindestens 10 Jahren aufbewahrt.

5.3.3 Statistische Auswertungen

Der Direktor SRK beauftragt ICT Services, statistische Auswertungen von Personengruppen, Abteilungen oder Departementen inkl. ASP-Kunden zu erstellen. Diese Auswertungen haben zum Ziel, die Hauptnutzergruppen zu lokalisieren, damit eine kontinuierliche Ausbauplanung unserer Kommunikationsinfrastruktur erfolgen kann. Die Auswertungen dienen zudem auch als Basis für die (interne) Leistungsverrechnung. Gleichzeitig helfen sie, Missbräuche aufzudecken. Die Departementsleiter und Verantwortlichen auf Seiten der ASP-Kunden erhalten auf Anfrage die Resultate der statistischen Auswertungen zur Information.

5.3.4 Personenbezogene Überwachung

Besteht auf Grund der statistischen Auswertungen gem. Ziff. 5.3.3 oder aufgrund anderer Hinweise der Verdacht auf Missbrauch der elektronischen Kommunikationseinrichtungen, informiert der Direktor resp. die Geschäftsleitung des ASP-Kunden die Mitarbeitenden, dass entsprechende Missbräuche vorgekommen sind, und dass im Wiederholungsfall die ICT Services mit einer personenbezogenen Auswertung beauftragt werden. Eine allfällige personenbezogene Auswertung muss zeitlich befristet und den Mitarbeitenden vorgängig angekündigt werden.

Die ICT Services übergeben die Auswertungsresultate dem berechtigten Auftraggeber. Die Resultate einer personenbezogenen Auswertung eines Mitarbeitenden eines ASP-Kunden werden dem Direktor SRK resp. der Geschäftsleitung des ASP-Kunden gemeldet.

Bei fehlbaren Mitarbeitenden sperrt ICT Services auf Anordnung des Direktors SRK resp. der Geschäftsleitung des ASP-Kunden den Zugang zu den Informatikinstrumenten vorsorglich. Zudem werden verdächtige Informationen zur späteren Auswertung durch die Anwaltschaft oder den Richter sichergestellt.

Es können Sanktionen gemäss Ziff. 5.3.5 ausgesprochen werden.

Beim Verdacht des Missbrauchs durch private E-Mails gelten die Ausführungen in Ziff. 5.1.9 und Ziff. 5.1.10.

5.3.5 Sanktionen

Werden im Rahmen der personenbezogenen Überwachung Verstösse festgestellt, hat die Direktion SRK oder die Geschäftsleitung des ASP-Kunden die Möglichkeit, gegen die Fehlbaren zivilrechtlich und strafrechtlich vorzugehen. Die Direktion SRK oder der ASP-Kunde kann alternativ oder kumulativ insbesondere folgende Sanktionen erheben:

- Verwarnung gegen die fehlbaren Personen
- Forderung von Schadenersatz
- Einreichung einer Strafanzeige

[2] grosser Internet-Zwischenspeicher

- Fristlose Kündigung

Die fristlose Kündigung kann in schwerwiegenden Fällen, wie bei wiederholtem Missbrauch trotz Verwarnung oder bei einer erwiesenen Straftat ausgesprochen werden. Die fristlose Kündigung kann ausgesprochen werden, wenn dem Arbeitgeber nach Treu und Glauben die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden kann (OR Art. 337 Abs. 2).

6 Umgang mit Smartphones und Tablets

6.1 Obligatorische Massnahmen

6.1.1 Bildschirmsperre

Obwohl eine Bildschirmsperre für einen Datendieb kein grosses Hindernis darstellt, hindert sie den Gelegenheitsdieb daran, über Ihr Abonnement zu telefonieren oder zu surfen und so Ihre Rechnung in die Höhe zu treiben.

- Sperren Sie den Bildschirm nicht nur mit der Tastensperre, sondern auch per Passwort! Stellen Sie die Option so ein, dass die Bildschirmsperre nach einer gewissen Zeit automatisch eingeschaltet wird.
- Verwenden Sie numerische PINs, die über die Tastatur eingegeben werden müssen. Vermeiden Sie Gesten, die auf dem Bildschirm gezeichnet werden müssen. Durch die Ablagerungen von Hautfetten auf dem Bildschirm können diese Muster einfach herausgefunden werden.
- Setzen Sie einen PIN mit 4 Zeichen oder mehr.

6.1.2 Antivirus

Mit der wachsenden Beliebtheit von Apps aus den Online Shop von Apple (iTunes), Google (Google Play) und Windows Phone (Marketplace) nimmt auch die Bedrohung durch Viren zu, die über diese Apps eingeschleust werden können. Die meisten Antiviren-Hersteller bieten inzwischen auch Antiviren-Software für alle gängigen Geräte und Plattformen von Smartphone und Tablets an. Beispiele für solche Softwares finden Sie im Anhang zu dieser Weisung.

- Installieren Sie auf dem Gerät eine Antivirus Software (siehe Anhang).
- Stellen Sie die Software so ein, dass sie sich durch regelmässige Updates immer aktualisiert.

6.1.3 Fernzugriff und –sperre

Wird Ihr Mobiltelefon trotz allen Vorsichtsmassnahmen gestohlen, ist es nur eine Frage der Zeit, bis ein Datendieb Ihre Schutzmechanismen geknackt hat und an Ihre Daten gelangt. Um dies zu verhindern, kann Ihr Mobiltelefon im Verlustfall über eine spezielle Software aus Distanz lokalisiert, gesperrt und Ihre Daten gelöscht werden. Beispiele für solche Softwares finden Sie im Anhang zu dieser Weisung.

- Installieren Sie eine Remote Access-Software auf dem Gerät.
- Erstellen Sie einen Account bei einem entsprechenden Anbieter, damit Sie Ihr Gerät im Verlustfall sofort sperren und löschen können.

6.1.4 Updates

Alle Online-Shops für Apps benachrichtigen Sie automatisch über Updates für die auf Ihrem Gerät installierten Apps.

- Installieren Sie Updates für Apps sobald als möglich

- Stellen Sie Ihr Gerät auch so ein, dass es regelmässig nach Updates für das Betriebssystem – iOS, Android, Windows Phone, etc. – sucht, und installieren Sie diese jeweils auch so rasch wie möglich.

6.1.5 Verlust sofort melden

Im Verlustfall gilt es nicht nur bei Kreditkarten, rasch zu handeln, um weiteren Schaden zu vermeiden. Je eher sie auf den Verlust des Smartphones reagieren, umso weniger Zeit hat ein Dieb, mit dem Gerät Schaden anzurichten.

- Wenn Ihr Smartphone oder Tablet gestohlen wird, melden Sie dies unbedingt sofort dem Service Desk und Ihrem Provider.
- Loggen Sie sich in die Fernwartung ein, sperren Sie Ihr Gerät und löschen Sie die Daten darauf.

6.1.6 iTunes, iCloud, Dropbox, SkyDrive etc.

Die Apple-Softwares iTunes und iCloud ermöglichen die Synchronisierung von Daten von iPhone zu PC, und von iPhone zu anderen iPhones oder iPads. Auf einem iTunes-Account können auch mehrere mobile Geräte zugefügt werden. Was in vielen Fällen sehr praktisch sein kann, hat aber auch seine Tücken! Ohne spezifisches Eingrenzen werden in iTunes und iCloud die Daten von einem Gerät auf alle Geräte synchronisiert. Wenn Sie also zum Beispiel Ihren SRK-Kalender in der iCloud freigeben, wird der auch auf die Geräte Ihrer Familienmitglieder synchronisiert. Ihre Kinder beispielsweise haben dann so Zugriff auf Ihre Termine und können diese auch irrtümlicherweise verändern, löschen oder Absagen senden!

- Trennen Sie Ihre geschäftlichen Daten von Ihren privaten Kalendern auf Google, Gmail oder ähnlichen Portalen.
- Synchronisieren Sie Ihre geschäftlichen Daten ausschliesslich über den offiziellen Kanal vom SRK.
- Legen Sie keine geschäftlichen Daten bei Cloud-Services wie z. B. Dropbox, iCloud, SkyDrive ab.

6.2 Empfohlene Massnahmen

6.2.1 Bluetooth

Bluetooth ist bei vielen Smartphone standardmässig eingeschaltet. Dadurch suchen die meisten Telefone laufend nach Geräten in Reichweite, mit denen sie Daten austauschen können. Diese Funktion belastet aber nicht nur Ihren Akku – viel schlimmer ist, dass ein Datendieb so nur auf wenige Meter an Ihr Gerät herankommen muss, um einen Virus einzuschleusen oder auf Ihrem Gerät herumzustöbern. Unsere Empfehlung:

- schalten Sie Bluetooth auf Ihrem Gerät nach Möglichkeit nur dann ein, wenn Sie es wirklich benötigen.
- wenn Sie Bluetooth dauernd eingeschaltet haben müssen, etwa zur Verbindung mit einem Headset, schalten Sie das Gerät auf „Unsichtbar“.
- stellen Sie das Gerät so ein, dass für jede aufgebaute Verbindung oder für jeden Datentransfer ein Passwort oder zumindest eine manuelle Bestätigung (<ja> = verbinde mein Gerät mit dem anderen) nötig ist.

6.2.2 Daten verschlüsseln

Viele Smartphones und Tablets bieten die Möglichkeit, die gespeicherten Daten zu verschlüsseln. So kann ein allfälliger Datendieb nicht einfach so auf die Daten zugreifen, ob er nun Ihr Gerät stiehlt oder über einen Virus auf Ihre Daten zugreifen will.

- Wenn Sie geschäftliche Daten auf Ihrem Gerät abspeichern, nutzen Sie die Verschlüsselung.

6.2.3 Backup

Die meisten Fernzugriff-Softwares bieten die Möglichkeit, auch ein Backup einzurichten. Aber auch beim Verbinden mit dem PC stellen die meisten Smartphones eine einfache Backup-Möglichkeit zur Verfügung. Mit regelmässigen Backups sind Sie im Verlust- oder Defektfall mit einem Ersatzgerät rasch wieder auf Ihrem aktuellen Datenstand.

- Machen Sie regelmässige Backups von Ihren Daten auf Ihren PC oder Apple zuhause.
- Prüfen Sie regelmässig, ob die Backups auch funktionieren, d.h. ob sie lesbar sind und sich auch zurückschreiben lassen.

6.2.4 Fremdes WLAN

Öffentliche WLAN Hotspots sind praktisch, weil sie eine wesentlich schnellere Verbindung ins Internet bieten als die Datenverbindung über das Funktelefonnetz und dabei gleichzeitig das Daten-Abo nicht belasten. Beachten Sie, dass solche öffentlichen WLAN Hotspots oft ungeschützt sind und Datendieben eine einfache Möglichkeit bieten, unverschlüsselte Daten auszuhorchen. Wir empfehlen:

- benutzen Sie über öffentliche WLAN Hotspots keine kritischen Anwendungen wie Online Banking, Einkauf per Kreditkarten oder ähnliches.
- verwenden Sie Seiten, bei denen Sie sich einloggen müssen nach Möglichkeit nur, wenn die Seite über **https** angeboten wird (verschlüsselte Seite). Im Browser wird dies durch einen farbig hinterlegten Teil der Adresszeile (Firefox) bzw. einem Symbol in Form eines Vorhängeschlosses angezeigt (Internet Explorer).
- laden Sie über öffentliche WLAN Hotspots keine Software zum Installieren herunter!
- verschicken Sie keine vertraulichen E-Mails über öffentliche WLAN Hotspots.

6.2.5 Datensynchronisation

Die SRK Infrastruktur bietet die Möglichkeit, E-Mails, Kalender und Notizen aus Outlook mit Smartphones oder Tablets zu synchronisieren. Sie können so direkt auf die entsprechenden Daten auf dem SRK-Server zugreifen und diese online bearbeiten. Dabei können Sie wählen, welche Bereiche Sie tatsächlich synchronisieren wollen.

- Synchronisieren Sie nur die Daten, die Sie auch wirklich verwenden.
- Stellen Sie Ihr Gerät so ein, dass nur Elemente der letzten 2 - 3 Tage in die Vergangenheit synchronisiert werden.

Beachten Sie, dass das Synchronisieren Ihr Abonnement belastet. Stellen Sie sicher, dass Sie eine entsprechende Flatrate oder ein Daten-Abonnement abgeschlossen haben.

Die vorliegende Weisung wurde erstmals von der Geschäftsleitung an ihrer Sitzung vom 12. Mai 1998 genehmigt und auf den 1. Juni 1998 in Kraft gesetzt. Die vorliegende, aktualisierte Version wird vom Direktor SRK genehmigt und in Kraft gesetzt.

Schweizerisches Rotes Kreuz

Der Direktor

Markus Mader

Bern, im April 2012