Ordnung für den Umgang mit IT-Systemen, IT-Services und Daten der SG Stern Deutschland e.V.

Inhalt

1. Einleitung

Ziel dieser Ordnung ist die einheitliche Regelung für den Umgang mit IT-Systemen, IT-Services und Daten sowie die Festlegung relevanter Verhaltensregeln. Im Folgenden sind mit IT-Systemen, IT-Services und Daten immer nur die des Vereins gemeint. Mit IT-Services sind zentrale Systeme in der Cloud (z.B. Microsoft Office 365) gemeint.

Die Ordnung dient dazu, den gesetzlichen Anforderungen gerecht zu werden, die vorgegebenen Sicherheitsstandards einzuhalten und Fehler im Umgang mit der IT zu minimieren, damit Informationssicherheit sowie Vertraulichkeit, Verfügbarkeit und Integrität der Systeme gewährleistet sind. Der Schutz dieser Informationen ist von existenzieller Bedeutung.

Die Ordnung regelt den Umgang mit allen Datenverarbeitungsgeräten (Infrastruktur, Netzwerk, Computer, Notebooks, Tablets, Smartphones, Peripheriegeräte, etc.) und IT-Services, die von der SG Stern Deutschland e.V. (nachfolgend als „Verein“ bezeichnet) bereitgestellt werden, privaten Datenverarbeitungsgeräten für die ehrenamtliche Tätigkeit und Datenverarbeitungsgeräten, die die Infrastruktur des Vereins nutzen.

Sie gilt für alle Beschäftigten und Ehrenamtlichen des Vereins. Zu den Beschäftigten gehören alle Festangestellten, Teilzeitangestellten, Auszubildende, Werkstudenten sowie Aushilfskräfte etc. Auch externe Personen (Übungsleiter, Honorarkräfte, etc.), die für den Verein tätig sind, sind verpflichtet, sich an diese Ordnung zu halten. Der Verein wird entsprechende Vorkehrungen treffen, damit diese Ordnung auch für die externen Personen verbindlichen Charakter hat.

Jeder Benutzer von IT-Systemen, IT-Services und Daten ist verpflichtet, geltende, einschlägige Gesetze und interne Regelungen zu beachten. Die Gesamtheit der Regelungen hat verbindlichen Charakter, sodass Verstöße gegen die Inhalte der Ordnung bei Beschäftigten zu arbeitsrechtlichen und bei Ehrenamtlichen zu privatrechtlichen Konsequenzen führen können.

Die Nutzung der Kommunikationssysteme unterliegt dem Telekommunikationsgesetz (TKG), dem Telemediengesetz (TMG), dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) und der EU-Datenschutz-Grundverordnung (DSGVO) i. V. m. dem Bundesdatenschutzgesetz (BDSG) in seiner ihren jeweils gültigen Fassungen.

Der Verein ist vom Gesetzgeber verpflichtet, in regelmäßigen Abständen die Einhaltung der Ordnung stichprobenartig zu überprüfen.

AGG Konformität: Sollte im Dokument aus Vereinfachungsgründen nur eine Geschlechtsform verwendet werden, ist ausdrücklich auch jede andere Geschlechtsform gemeint.

2. Benutzer-Verantwortlichkeiten

2.1 Grundlagen der Nutzung

Zur Gewährleistung der Informationssicherheit sowie der Vertraulichkeit, Verfügbarkeit und Integrität der Systeme, ist unzulässig:

(1) Die Nutzung der IT-Systeme, IT-Services und Daten in einer Art, die
   a) gegen die jeweils gültigen Gesetze verstößt
   b) gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt
   c) für den Verein geschäftsschädigend ist
   d) beleidigende, diskriminierende, verleumderische, bedrohende, verfassungsfeindliche, rassistische, sexistische, obszöne, sexuell orientierte, pornografische, diffamierende oder anderweitig anstößige Inhalte aufweist oder diese kommuniziert (Belästigungen und Diskriminierungen können bereits unter Bezugnahme auf Geschlecht, Rasse (einschließlich Hautfarbe, Nationalität oder ethnischer oder nationaler Herkunft), Alter, sexueller Orientierung, Familienstand, religiöser Überzeugung und Behinderung auftreten)
   e) weltanschauliche, religiöse oder parteipolitische Inhalte hat
   f) der Erzielung von persönlichen finanziellen oder kommerziellen Gewinnen einschließlich Werbung dient.

(2) Der unberechtigte Zugriff auf Computer, Smartphones, Notebooks, Tablets oder andere Geräte, Dateien, Daten, Voicemails oder E-Mails anderer Personen.

(3) Die nicht wahrheitsgemäße und nicht präzise Identifikation sowie die Vortäuschung einer falschen Identität.

(4) Die Verwendung der IT-Systeme, IT-Services und Daten des Vereins, um Unbefugten Zugriff auf Datenverarbeitungsgeräte des Vereins oder IT-Systeme, IT-Services und Daten anderer Vereine zu verschaffen.

(5) Aktivitäten, die den bestimmungsgemäßen Betrieb der IT-Systeme, IT-Services und Daten beeinträchtigen oder die Informationssicherheit gefährden.

(6) Die öffentlichkeitswirksame Registrierung des Namens des Vereins/der Marke auf einer Internetseite oder bei einem anderen elektronischen IT-Service ohne vorherige Zustimmung einer bevollmächtigten Stelle (mit Ausnahme der Nennung des Arbeitsgebers in persönlichen Profilen sozialer Netzwerke). Erlaubt ist lediglich die Anlage von Accounts, bei denen die Angabe des Namens des Vereins inkl. Adresse geschäftlich veranlasst und aus kaufmännischen bzw. technischen Gründen notwendig ist.

(7) Beim Betrieb von privaten Internetseiten, Blogs, Foren, Chats und Profilen in sozialen Netzwerken:
   a) Die negative Darstellung des Vereins, seiner Beschäftigten sowie Ehrenamtlichen und damit die Gefährdung des guten Rufs
   b) Die Offenlegung von geschützten oder vertraulichen Informationen (siehe auch die jeweils aktuelle Richtlinie zu Insiderinformationen).
   c) Die Verletzung von Sicherheitsbestimmungen oder anderer anwendbarer Gesetze

(8) Darüber hinaus ist mit den durch den Verein bereitgestellten Endgeräten sorgfältig, sachgemäß und werterhaltend umzugehen. Beim Transport sind die Geräte in geeigneten gepolsterten Taschen oder Rucksäcken zu verstauen oder mit geeigneten Schutzhüllen zu versehen. Beim Transport im Auto oder öffentlichen Verkehrsmitteln sind die Geräte so zu verstauen, dass sie sich beeinflusst durch das Verkehrsgeschehen nicht unkontrolliert im Fahrzeug bzw. Verkehrsmittel bewegen können. Die Geräte sind regelmäßig mit geeigneten Utensilien zu reinigen (z.B. Microfasertuch für Touchscreens, KEINE Feuchttücher für Touchscreens).

2.2 Geschäftliche Nutzung von Endgeräten und IT-Services des Vereins

(1) Bei Daten oder Software, die vom Verein gekauft, gemietet, entwickelt oder erstellt wurden, sind Bestimmungen des Urheberrechts- und Lizenzbedingungen zu beachten. Die Weitergabe an Dritte ist nur im Sinne der Geschäftszwecke des Vereins und in Übereinstimmung mit den geltenden Lizenzbedingungen zulässig. Voraussetzung ist, dass die geltenden Lizenzbedingungen eine Weitergabe gestatten.

(2) Bei Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden, ist die eigenmächtige Installation und jede Veränderung von System- oder Anwendungssoftware unzulässig. Bei Bedarf muss die IT kontaktiert werden. Diese entscheidet über das weitere Vorgehen. Die Benutzung privater oder nicht lizenzierter Softwarekopien auf Firmen-PCs ist unzulässig.

(3) Bei Bedarf an neuer Software für die geschäftliche Nutzung ist von der IT zu prüfen, ob Alternativen oder bereits bestehende Lizenzverträge vorhanden sind.

(4) Sobald ein Fehler oder ein anderes Problem mit Beeinträchtigung des bestimmungsgemäßen Betriebs der IT-Systeme, IT-Services und Daten oder Gefährdung der Informationssicherheit auftreten, ist unverzüglich die IT zu benachrichtigen.

(5) Das Auftreten von Viren oder Schadcode ist unverzüglich der IT per Telefon und E-Mail zu melden.

(6) Hardware, die vom Verein zur Verfügung gestellt wird, darf mit Ausnahme von Auftragsarbeiten (z.B. für externe Beschäftigte, externe Berater, etc.) nur selbst genutzt werden.

(7) Mit der vom Verein zur Verfügung gestellten Hardware ist fürsorglich und sachgemäß umzugehen.

(8) Bei Verlust von Notebooks, Smartphones, Speichermedien oder Zutrittskarten/Schlüssel ist dieser unverzüglich dem zuständigen Vorgesetzten und der IT zu melden. Gleiches gilt für den Verdacht unberechtigter Benutzung oder Manipulation des PCs/Notebooks oder Smartphones durch Dritte. Die IT hat ggf. sofort den Zugang zu sperren bzw. das Gerät zu deaktivieren. Die Meldung hat auch zu erfolgen, wenn private Datenverarbeitungsgeräte für die ehrenamtliche Tätigkeit für den Verein verloren gehen, gestohlen werden oder ein unberechtigter Zugriff stattgefunden hat. Wenn das Gerät wieder aufzufinden sein sollte, ist dieses vor dem erneuten Einsatz auf Manipulation oder Schadcode von der IT untersuchen zu lassen (Keylogger, Malware, Logfiles etc.), bevor das Gerät wieder auf die vom Verein bereitgestellten Dienste zugreift.

(9) Bei Sicherheitsvorfällen ist den Anweisungen der IT Folge zu leisten.

(10) Bei Verlassen des Arbeitsplatzes bzw. Unterbrechung oder Beendigung aktueller Arbeiten, sind Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden (PC, Notebook,

Smartphone, Tablet etc.) gegen fremden Zugriff zu sperren („STRG+ALT+ENTF und Sperren“ oder Windows+L) und bei Nutzung privater Datenverarbeitungsgeräten für die ehrenamtliche Tätigkeit die für den Verein genutzten IT-Services und Daten gegen fremden Zugriff zu sperren. Eine automatische Sperrung bei Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden, erfolgt gemäß der jeweils aktuellen Einstellung der Gruppenrichtlinie der Domäne.

(11) Am Ende des Arbeitstages sind Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden, mit Ausnahme des Smartphones herunterzufahren oder auszuschalten. Ausnahmen gelten bei automatisierten Verarbeitungen auf dem PC, die über das Arbeitsende hinausgehen, oder bei Systemen, die permanent IT-Services bereitstellen (Druckserver, Fileserver etc.).

(12) Bei Zugriff auf E-Mails oder auf das Netzwerk des Vereins außerhalb der Geschäftsräume ist darauf zu achten, dass personenbezogene oder vertrauliche Daten nicht automatisch mitgespeichert und nicht von Unbefugten eingesehen werden können.

(13) Gästen/Besuchern von Geschäftsstellen ist ausschließlich der Zugang zum angebotenen WLAN für Gäste/Besucher zu ermöglichen. Gäste/Besucher, die das bereitgestellte WLAN nutzen möchten, werden darauf hingewiesen oder bestätigen, dass sie das angebotene WLAN ausschließlich für berufliche Zwecken nach den geltenden Gesetzen des jeweiligen Standorts nutzen und die Nutzung zur Sicherstellung der Informationssicherheit protokolliert und im Bedarfsfall ausgewertet wird. Sofern der Gast/Besucher Zugang zu internen IT-Services und Systemen benötigt, darf dies nur über durch den Verein bereitgestellte Endgeräte erfolgen.

(14) Der Aufbau umfangreicher benutzereigener Verfahren (Programme, Skripte, Excel-Sheets, Access-Datenbanken, etc.) ist nur im Einvernehmen mit dem jeweiligen Vorgesetzten oder der IT zugelassen. Ebenfalls ist eine Meldung an den Datenschutzkoordinator oder Datenschutzbeauftragten mittels Formular zur Meldung eines neuen Verfahrens zur Datenverarbeitung vorzunehmen. Die Verfahren sind so zu dokumentieren, dass ein sachverständiger Dritter in angemessener Zeit die Nutzung und Pflege der Programme übernehmen kann.

(15) Die dem Beschäftigten bereitgestellten Endgeräte werden von der IT dokumentiert.

2.3 Private Nutzung von Endgeräten und IT-Services des Vereins

(1) Die durch den Verein bereitgestellten Geräte (Computer, Notebooks, Tablets, Smartphones (Telefonie und Datennutzung)), IT-Systeme (Netzwerk inkl. WLAN, Server, Peripherie, etc.) und IT-Services sind primär für die geschäftliche Nutzung vorgesehen. Die private Nutzung von Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden, ist unter Berücksichtigung der Grundlagen für die Nutzung gem. Ziffer 2.1. in geringfügigem Umfang während der Pausen und außerhalb der Arbeitszeit gestattet sofern dies nicht zu einer Beeinträchtigung der geschäftlichen Nutzung führt. Mittels Stichproben überprüft die IT, ob die Restriktion eingehalten wird. Sämtlicher Datenverkehr wird seitens des Vereins protokolliert.

(2) Die Nutzung der IT-Systeme, IT-Services und Daten über private Geräte (Bring Your Own Device (BYOD)) ist untersagt. Ausgenommen hiervon sind IT-Services des Vereins, die über die Cloud abgerufen werden, keine Daten auf private Endgeräte synchronisieren und damit die Datenhoheit beim Verein bleibt (z.B. Microsoft Office 365). Sofern die Bearbeitung von Dokumenten über die Cloud ohne die lokale Synchronisation nicht möglich ist, ist der temporäre Download auf das private Endgerät und die lokale Bearbeitung unter der Voraussetzung

gestattet, dass das Dokument nach Bearbeitung wieder auf eine der Datenhoheit des Vereins zugehörige Infrastruktur übertragen und auf dem privaten Endgerät gelöscht wird. Auch der Anschluss privater Geräte (bspw. private externe Festplatte oder USB-Stick) an die IT-Infrastruktur des Vereins ist mit Ausnahme der privaten Endgeräte, die durch die IT nachweislich genehmigt wurden (mindestens in Textform) und damit den Richtlinien des Vereins unterliegen, untersagt. Weitere Ausnahmegenehmigungen erfolgen auf Antrag durch die Geschäftsleitung.

(3) Heimarbeitsplätze für Beschäftigte (Nutzung privater Endgeräte für die Wahrnehmung geschäftlicher Aufgaben) werden seitens des Vereins nicht zur Verfügung gestellt. Daher ist die Nutzung geschäftlicher IT-Services des Vereins über private Endgeräte und/oder private Infrastrukturen ebenfalls untersagt. Ausgenommen hiervon sind IT-Services des Vereins, die über die Cloud abgerufen werden, keine Daten auf private Endgeräte synchronisieren und damit die Datenhoheit beim Verein bleibt (z.B. Microsoft Office 365). Weitere Ausnahmegenehmigungen erfolgen auf Antrag durch die Geschäftsleitung.

(4) Bei der Heimarbeit oder dem mobilen Arbeiten von Beschäftigten sind ausschließlich die vom Verein bereitgestellten Geräte (Computer, Notebooks, Tablets, Smartphones (Telefonie und Datennutzung)) zu verwenden (Peripheriegeräte ohne Datenhaltung ausgenommen). Die Datenhoheit muss zu jeder Zeit beim Verein liegen. Die Nutzung geschäftlicher IT-Services des Vereins über private Endgeräte ist untersagt. Die Nutzung der privaten Infrastruktur (Internetzugang) ist gestattet. Ausgenommen hiervon sind IT-Services des Vereins, die über die Cloud abgerufen werden, keine Daten auf private Endgeräte synchronisieren und damit die Datenhoheit beim Verein bleibt (z.B. Microsoft Office 365). Weitere Ausnahmegenehmigungen erfolgen auf Antrag durch die Geschäftsleitung.

(5) Software, die vom Verein gekauft, gemietet, entwickelt oder erstellt wurde, darf in geringfügigem Umfang während der Pausen und außerhalb der Arbeitszeit privat genutzt werden, sofern damit keine Lizenzbestimmungen oder geltende Gesetze verletzt werden und keine zusätzlichen nutzungsabhängigen Gebühren oder Transaktionskosten entstehen.

(6) Die Installation privater Software auf Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden, ist untersagt.

(7) Daten, die vom Verein gekauft, gemietet, entwickelt oder erstellt wurden, dürfen nicht privat genutzt werden.

(8) Private Daten dürfen nicht auf einem zentralen Speichersystem des Vereins (z.B. SharePoint, OneDrive, Shares, etc.), sondern nur auf den jeweils bereitgestellten Endgeräten vorgehalten werden (ohne Einschränkung der für geschäftliche Zwecke benötigten Speicherkapazität). Für die Datensicherung dieser privaten Daten ist ausschließlich der Beschäftigte und Ehrenamtliche verantwortlich. Der Verein übernimmt keine Haftung bei Verlust von privaten Daten. Bei einer Verschlüsselung der Endgeräte durch den Verein werden eventuell auch private Daten des Beschäftigten verschlüsselt. Bei notwendigem Zugriff des Vereins auf Endgeräte, die der Verein bereitgestellt hat, ist nicht auszuschließen, dass private Daten zur Kenntnis genommen werden. Vor Austausch des Endgeräts hat der Beschäftigte die Möglichkeit, private Daten zu löschen. Der Verein kann vor Austausch des Endgeräts oder bei Notwendigkeit zu einem anderen Zeitpunkt ein Backup anfertigen. Nicht gelöschte private Daten werden Teil des Backups, ein Anspruch auf Löschung des Backups hat der Beschäftigte nicht.

(9) Durch den Verein bereitgestellte Geräte verbleiben trotz erlaubter Privatnutzung auch bei Austritt des Beschäftigten im Eigentum des Vereins.

(10) Wird ein durch den Verein bereitgestelltes Gerät auf Basis einer separaten Regelung privat übernommen, erfolgt im Bedarfsfall die vollständige Löschung des Endgeräts vor Übergabe.

(11) Auch bei wiederholter, vorbehaltloser Gewährung der Privatnutzung entsteht kein Rechtsanspruch auf Gewährung für die Zukunft.

(12) Der Verein muss die gesetzlichen Aufbewahrungspflichten erfüllen. Soweit sich aufgrund der privaten Nutzung von Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden, unter den geschäftlichen Daten auch private Daten des Beschäftigten befinden, ist dem Beschäftigten bewußt, dass die Speicherung dieser anfallenden privaten personenbezogenen Daten erfolgt. Sofern dies nicht gewünscht wird, ist ihm die Privatnutzung untersagt. Gleiches gilt für das E-Mail Postfach des Vereins oder den Clouddiensten bei Nutzung privater Datenverarbeitungsgeräten für die ehrenamtliche Tätigkeit für den Verein.

2.4 Telefonie und mobile Datenverbindungen

(1) Alle durch den Verein bereitgestellten mobilen Endgeräte (Smartphones) verfügen über eine Dual SIM Funktion. Beschäftigte können das dienstliche Smartphone nur geschäftlich nutzen und daher von der Dual SIM Funktion keinen Gebrauch machen oder das Gerät geschäftlich und privat und damit die Dual SIM Funktion nutzen.

(2) Für die Telefoniefunktion und die Datenverbindung via Mobilfunkbetreiber ist die Privatnutzung über die private Dual SIM Karte unbeschränkt sowie für die Telefoniefunktion über lokale Telefone/Telefoniedienste des Vereins in geringfügigem und angemessenem Umfang unter Berücksichtigung anfallender Kosten gestattet. Die geschäftlich veranlasste Privatnutzung (z.B. Mitteilung an Familie und familiennahe Kontakte, dass sich die Heimkehr verzögert) ist grundsätzlich als dienstliche Nutzung anzusehen. Sämtliche Telefonieverbindungen und der Datenverkehr werden seitens des Vereins protokolliert.

(3) Sofern über die geschäftliche Rufnummer Telefonie- und Datenverbindungen genutzt werden, deren Gebühren nicht über die Flatrate gedeckt sind, sind die Kosten gem. Einzelverbindungsnachweis vom Beschäftigten zu tragen. Die dafür notwendigen Einzelverbindungsnachweise dürfen folgende Angaben enthalten: Rufnummer ausgehend, Zielrufnummer, Datum des Gesprächs, Uhrzeit des Gesprächs, Dauer des Gesprächs, Verbindungspreis. Für die Nutzung der Einzelverbindungsnachweise gilt §99 Telekommunikationsgesetz (TKG).

(4) Auch bei wiederholter, vorbehaltloser Gewährung der Privatnutzung entsteht kein Rechtsanspruch auf Gewährung für die Zukunft.

(5) Der Verein muss die gesetzlichen Aufbewahrungspflichten erfüllen. Soweit sich aufgrund der privaten Nutzung unter den geschäftlichen Daten auch private Daten des Beschäftigten befinden, erfolgt die Speicherung dieser anfallenden privaten personenbezogenen Daten. Sofern dies nicht gewünscht wird, ist ihm die Privatnutzung untersagt.

2.5 Datenhaltung und Datenübertragung

(1) Sämtliche geschäftsrelevante Daten sind ausschließlich auf einem vom Verein bereitgestellten Endgerät, einem zentralen Speichersystem oder einem externen IT-Service abzulegen, um einen Datenverlust vorzubeugen. Sofern durch den Verein keine andere Methode oder

technische Maßnahme vorgegeben ist, hat der Transfer mittels gesicherter Verbindung (VPN) oder direkt über den bereitgestellten Clouddienst (Microsoft Office 365) zu erfolgen. Die Speicherung von Daten, die für den oder vom Verein erstellt worden sind, auf nicht vom Verein bereitgestellten oder freigegebenen Speichersystemen ist nicht gestattet. Die Datenspeicherung in nicht durch den Verein freigegebenen Clouddiensten ist ebenfalls nicht gestattet. Auch ist die Datenübermittlung über nicht durch den Verein freigegebene Clouddienste untersagt. Sofern die Bearbeitung von Dokumenten über die Cloud ohne die lokale Synchronisation nicht möglich ist, ist der temporäre Download auf das private Endgerät und die lokale Bearbeitung unter der Voraussetzung gestattet, dass das Dokument nach Bearbeitung wieder auf eine der Datenhoheit des Vereins zugehörige Infrastruktur übertragen und auf dem privaten Endgerät gelöscht wird. Darüber hinaus sind alle geschäftsrelevanten Datenträger, die personenbezogene Daten beinhalten, gegen Diebstahl zu schützen, vor allem bei Reisetätigkeit.

(2) Für den Austausch von Dokumenten mit Dritten ist auf dem durch den Verein bereitgestellten Clouddienst (Microsoft Office 365) eine SharePoint Seite „Spartenaustausch“ eingerichtet. Dritte sind alle Personen, die nicht hauptamtlich für den Verein tätig, oder (ehrenamtliche) Mitglieder des Vereins sind. Über diese Ressource können Dokumente auch mit Dritten geteilt werden. Bitte beachten Sie, dass über diese Ressource ausschließlich Inhalte bereitgestellt werden dürfen, für die seitens der Betroffenen eine gültige Einwilligung zur Veröffentlichung der personenbezogenen Daten vorliegt. Dazu zählen z. B. Fotos, für deren Veröffentlichung die jeweils abgebildeten Betroffenen eine Einwilligung erteilt haben. Auf dieser Ressource dürfen keine Dokumente veröffentlicht werden, die über das Bild hinaus weitere personenbezogene Daten enthalten.

(3) Bei der Arbeit ohne Verbindung zum Netzwerk (Offline-Arbeit) sind die Daten zeitnah und regelmäßig auf ein Speichersystem des Vereins zu übertragen. Sofern durch den Verein keine andere Methode oder technische Maßnahme vorgegeben ist, hat der Transfer mittels gesicherter Verbindung (VPN) oder direkt über den bereitgestellten Clouddienst (Microsoft Office 365) zu erfolgen. Bei Verlust (Abhandenkommen, Diebstahl, etc.) oder Defekt eines Geräts des Vereins (Notebook, Computer, Smartphone, Tablet, Speicher) bzw. einem privat genutzten Endgerät mit Daten des Vereins, soll auf keinen Fall mehr als die Arbeit eines Tages verloren gehen. Dies liegt in der Verantwortung jedes Beschäftigten und Ehrenamtlichen.

(4) Die lokale Speicherung von Daten (z.B. auf dem „Desktop“, im Ordner „Eigene Dokumente“, etc.) ist nur zulässig, wenn die Daten zeitnah und regelmäßig auf ein Speichersystem des Vereins übertragen werden.

(5) Redundante Datenhaltung auf den Speichersystemen ist zu vermeiden.

(6) Die Übertragung bzw. die Synchronisation von Daten des Vereins oder der Mitglieder (z.B. zwischen Notebook und Smartphone) darf nur zwischen Endgeräten oder Clouddienst (Microsoft Office 365) erfolgen, die seitens des Vereins bereitgestellt werden (mit Ausnahme der privaten Endgeräte, die durch die IT nachweislich genehmigt wurden (mindestens in Textform) und damit Richtlinien des Vereins unterliegen).

(7) Der Versand von personenbezogenen oder vertraulichen Daten über öffentliche Netzwerke hat ausschließlich verschlüsselt (z.B. Azure Information Protection [AIP], Data Loss Protection [DLP]) zu erfolgen.

(8) Der Versand von besonderen personenbezogenen oder vertraulichen Daten (Informationen über Gehälter, Dienstbeurteilungen, etc.) über interne Netze hat ausschließlich verschlüsselt (z.B. Azure Information Protection [AIP], Data Loss Protection [DLP]) zu erfolgen.

(9) Nicht mehr benötigte Informationsträger (Ausdrucke) mit personenbezogenen oder vertraulichen Informationen sind datenschutzkonform in einem Aktenvernichter oder in dafür vorgesehen Behältnissen zu vernichten.

(10) Ausdrucke von personenbezogenen oder vertraulichen Dokumenten an nicht zugriffsgeschützten Druckgeräten (z.B. mittels Passworteingabe/Chipkarte) sind unverzüglich nach Ausdruck am Drucker abzuholen.

2.6 Umgang mit Passwörtern

(1) Persönliche Passwörter (z.B. Login, interne Systeme, Zugänge zu Systemen oder Software von externen Anbietern, etc.) für Datenverarbeitungsgeräten oder IT-Services, die durch den Verein bereitgestellt werden, sind gegen unbefugte Nutzung zu sichern (z.B. mittels LastPass) und niemandem mitzuteilen.

(2) Sofern Passwörter nicht durch die Systeme vorgegeben sind, sind für den Zugang zu Systemen mit personenbezogenen oder vertraulichen Informationen Passwörter mit einer Mindestlänge von sechs Zeichen zu vergeben. Darüber hinaus werden alphanumerische Passwörter (Groß- und Kleinbuchstaben) und Zahlen) sowie ggf. folgende Sonderzeichen empfohlen: # $ & - ! ? % = : ( ).

(3) Sofern Gruppen-Accounts zwingend erforderlich sind und keine technischen Maßnahmen möglich sind, die eine Bekanntgabe des Passwortes an alle Gruppenmitglieder verhindern, gilt:

- Gruppenpasswörter sind umgehend zu ändern, wenn ein Mitglied der Gruppe den Verein verlässt oder unautorisierten Personen das Passwort bekannt geworden ist.
- unabhängig davon ist eine regelmäßige Änderung des Passwortes alle 180 Tage vorzunehmen.
- bei System- oder Datenveränderungen mittels eines Gruppen-Accounts ist eine separate Protokollierung sicherzustellen, welche eine Zuordnung der Änderung zu einer physischen Person ermöglicht.
- Für die Vergabe von Gruppenpasswörtern gelten die gleichen Kriterien wie für persönliche Passwörter (siehe 2.6 Absatz 2)

(4) Sofern eine Übermittlung von Passwörtern erforderlich ist, sind geeignete Schutzmaßnahmen zu treffen, die eine unbefugte Verwendung oder unbeabsichtigte Bekanntgabe des Passwortes wirksam verhindern. Eine gleichzeitige Übermittlung von Account-Bezeichnung und zugehörigem Passwort über denselben Kommunikationskanal ist unzulässig.

2.7 Informationssicherheit

(1) Durch den Verein bereitgestellte Datenverarbeitungsgeräte sind manuell zu sperren („STRG+ALT+ENTF und Sperren“ oder Windows+L), wenn diese für kurze Zeit unbeaufsichtigt sind. Bei Nutzung privater Datenverarbeitungsgeräten für die ehrenamtliche Tätigkeit sind die für den Verein genutzten IT-Services zu sperren.

(2) Die Einsicht für Unbefugte auf Computer, Notebooks, Smartphones, Tablets oder andere Geräte und damit die Einsicht in Inhalte und E-Mail Nachrichten oder Kenntnisnahme von Sprachnachrichten, mit Bezug zum Verein, ist zu verhindern. Dies kann am besten damit erreicht werden, indem der Zugriff auf die Geräte oder IT-Services nicht in direkter Anwesenheit Unbefugter vorgenommen wird bzw. das Gerät für die Einsichtnahme und den Zugriff durch Unbefugte gem. Abs. 1 gesperrt ist. Bei Smartphones ist die Nachrichtenvorschau mit Bezug zum Verein auf dem Sperrbildschirm zu deaktivieren.

(3) Für jegliche Unterlagen in Papierform (Ordner, Rechnungen, Mitgliedsdaten usw.), muss die Datenhoheit stets beim Verein liegen.

(4) Erfordern die betrieblichen Abläufe die Mitnahme oben genannter Unterlagen, so ist dies in einer auf dem SharePoint abgelegten Liste zu dokumentieren.

2.8 Mobiles Arbeiten für Beschäftigte des Vereins

Beim mobilen Arbeiten ist wie folgt zu beachten:

(1) Sicherung der häuslichen Arbeitsräume: Der Mitarbeiter hat dafür zu sorgen, dass der Raum/die Räume, in denen die häusliche Telearbeit durchgeführt wird, für die Dauer der Telearbeit nicht von unbefugten Dritten betreten werden können. Es sind geeignete Maßnahmen zu treffen, die den unbefugten Zugriff auf die Arbeitsmittel, Daten oder Dokumente verhindern (z.B. Sperrung des Arbeitsrechners etc.).

(2) Sichtschutz: Der Mitarbeiter hat dafür zu sorgen, dass unbefugte Dritte keine dienstlichen Dokumente und Daten einsehen können. Er hat insbesondere dafür zu sorgen, dass der Arbeitsbildschirm von Laptops oder Dokumenten nicht „im Vorbeigehen“ einsehbar ist (Sichtschutzfolien oder Einschränkung der Sicht auf Bildschirme).

(3) Akustischer Schutz: Der Mitarbeiter hat sicherzustellen, dass dienstliche Gespräche nicht von unbefugten Dritten mitgehört werden können. Er hat insbesondere dafür zu sorgen, dass am Telearbeitsplatz keine akustischen Assistenzsysteme (z.B. Alexa) vorhanden sind.

(4) Nutzung Internetzugänge: Der Mitarbeiter hat den eigenen privaten Internetzugang für die Telearbeit in geeigneter Weise zu sichern.

(5) Datensicherung: Der Mitarbeiter muss Daten, stets entsprechend der Vorgaben des Vereins, sichern. Werden Daten lokal auf den Arbeitsmitteln gespeichert, sind sie bei nächster Gelegenheit auf Datenspeicher zu übertragen, die der Verein üblicherweise für die Speicherung von Daten verwendet.

(6) Zugangsrecht: Der Mitarbeiter hat dem Verein oder dessen Mitarbeitern - nach vorheriger Absprache - Zugang zu seiner häuslichen Arbeitsstätte zu gewähren. Dies ist insbesondere dann der Fall, wenn die Einhaltung dieser Vereinbarung kontrolliert werden muss oder die Einhaltung datenschutzrechtlicher Bestimmungen geprüft werden soll (zum Beispiel durch den Datenschutzbeauftragten des Vereins). Der Zugang ist nur zu den gängigen Geschäftszeiten (z. B. zwischen 10:00 Uhr und 17:00 Uhr) zu gewähren. In dringenden Fällen muss der Zugang ohne vorherige Absprache gewährt werden. Die Grundrechte und Grundfreiheiten der Mitarbeiter und der Schutz der häuslichen Privatsphäre sind stets einzuhalten.

(7) Weisungen: auch beim mobilen Arbeiten hat sich der Mitarbeiter an die Weisungen des Arbeitgebers zu halten.

3. Internet und E-Mail Nutzung

3.1 Nutzung des E-Mail Postfachs des Vereins

(1) E-Mails mit personenbezogenen oder vertraulichen Informationen dürfen nur befugten Personen (z.B. über Stellvertreterregelung) bekannt gegeben, offengelegt oder weitergeleitet werden.

(2) Die Weiterleitung von E-Mail Adressen oder E-Mail Nachrichten des Vereins an private E-Mail Adressen ist untersagt, sofern diese Privatnutzung nicht als dienstliche Nutzung anzusehen und damit eine geschäftlich veranlasste Privatnutzung ist.

(3) Die Nutzung der E-Mail Adresse des Vereins zur Anmeldung für ausschließlich privat genutzte Accounts und Portale ist untersagt.

(4) Auf Anordnung der Geschäftsleitung kann aus wichtigen geschäftlichen Gründen Zugriff auf das E-Mail Postfach des Vereins erfolgen.

(5) Bei eingehenden E-Mails ist sorgfältig zu prüfen, ob Integrität, Vertraulichkeit und Authentizität der Absender und Inhalte gegeben sind. Bei Unsicherheit dürfen ohne Rücksprache mit der IT keine Anhänge geöffnet oder betroffene E-Mails weitergeleitet werden.

(6) Für Zwecke des Vereins ist die Nutzung privater E-Mail Adressen untersagt.

(7) Sofern die E-Mail Adresse des Vereins für die Bearbeitung von E-Mail Nachrichten im lokalen E-Mail Programm eingebunden ist bzw. die Arbeit mit dem E-Mail Account ohne die lokale Synchronisation nicht möglich ist, ist der temporäre Download auf das private Endgerät und die lokale Bearbeitung unter der Voraussetzung gestattet, dass der E-Mail Account nach Beendigung der Tätigkeit für den Verein wieder auf eine der Datenhoheit des Vereins zugehörige Infrastruktur übertragen und inkl. dem Datenbestand (vorhandene E-Mails) auf dem privaten Endgerät gelöscht wird.

(8) Der Inhalt von E-Mails und deren Anlagen im E-Mail Postfach des Vereins sind vertraulich und ausschließlich für den bezeichneten Adressaten bestimmt. Bei Empfang von E-Mails, bei denen der Beschäftigte nicht der vorgesehene Adressat der E-Mail oder dessen Vertreter ist oder bei Versand von E-Mails an den falschen Adressaten oder dessen Vertreter ist jede Form der Kenntnisnahme, Veröffentlichung, Vervielfältigung oder Weitergabe des Inhalts der E-Mail auf Seiten des falschen Empfängers unzulässig. Ein solcher Vorfall ist der IT zu melden.

(9) Elektronische Datenübertragung ist im Hinblick auf Vertraulichkeit und Authentizität unsicher und trotz Sicherheitsvorkehrungen lässt sich die Übermittlung von so genannten Computerviren oder Trojanern nicht mit hinreichender Sicherheit ausschließen.

3.2 Nutzung des Internets

(1) Bei der Verwendung von Informationen, die über das Internet abgerufen werden, ist mit Sorgfalt vorzugehen, da Integrität, Vertraulichkeit und Authentizität der Informationen nicht gesichert sind. Daher kann nicht garantiert werden, dass die betreffenden Informationen richtig, genau oder vollständig sind.

3.3 Private Nutzung des Internets für Beschäftigte des Vereins

(1) Der vom Verein bereitgestellte Internetzugang ist primär für die geschäftliche Nutzung vorgesehen, die private Nutzung ist unter Berücksichtigung der Grundlagen für die Nutzung gem. Ziffer 2.1. in geringfügigem Umfang, während der Pausen und außerhalb der Arbeitszeit gestattet, sofern dies nicht zu einer Beeinträchtigung der geschäftlichen Nutzung führt. Gleiches gilt für die Nutzung des Internets zu privaten Zwecken über ein vom Verein bereitgestelltes internetfähiges Endgerät außerhalb des Vereins.

Die geschäftlich veranlasste Privatnutzung (z.B. Mitteilung an Familie und familiennahe Kontakte, dass sich die Heimkehr verzögert) ist grundsätzlich als dienstliche Nutzung anzusehen.

(2) Auch bei wiederholter, vorbehaltloser Gewährung der Privatnutzung entsteht kein Rechtsanspruch auf Gewährung für die Zukunft.

(3) Der Verein muss die gesetzlichen Aufbewahrungspflichten erfüllen. Soweit sich aufgrund der privaten Nutzung unter den geschäftlichen Daten auch private Daten des Beschäftigten befinden, erfolgt die Speicherung dieser anfallenden privaten personenbezogenen Daten. Sofern dies nicht gewünscht wird, ist ihm die Privatnutzung untersagt.

3.4 Private Nutzung des E-Mail Postfachs des Vereins

(1) Die Nutzung des vom Verein bereitgestellten E-Mail Postfachs und E-Mail Clients (lokal, über mobile Endgeräte oder Outlook Web Access) zu privaten Zwecken ist sowohl über IT-Equipment des Vereins als auch private Endgeräte untersagt.

3.5 E-Mail Archivierung

(1) Der Verein setzt wegen gesetzlicher Vorschriften zu Aufbewahrungsfristen und aus Sicherheitsgründen eine Technik zur Archivierung aller E-Mails im Originalzustand ein. Damit werden alle eingehenden und versendeten E-Mails ungeachtet der Bearbeitung im jeweiligen Postfach des Vereins im Originalzustand im E-Mail Archiv gespeichert. Darüber hinaus werden alle von außen eingehenden E-Mails an funktionsbezogene Adressen mit Absender, Empfänger, E-Mail-ID, Datum und Uhrzeit in einer Log-Datei gespeichert.

(2) Dem Beschäftigten oder Ehrenamtlichen ist bekannt, dass vorhandene private E-Mails oder E-Mails, die unbeabsichtigt empfangen worden sind, Teil des E-Mail Archivs sind. Archivierte E-Mails mit persönlichen Daten können nicht einzeln gelöscht werden, ein Widerrufsrecht kann daher nicht eingeräumt werden.

3.6 Datenerfassung

(1) Der Verein protokolliert zur Erfüllung gesetzlicher Vorgaben und zur Sicherstellung der Informationssicherheit alle Zugriffe auf die IT-Systeme, IT-Services und Daten, speichert und wertet diese bei Bedarf aus.

(2) Die bei der Nutzung der IT-Systeme, IT-Services, E-Mail-, Internet-, und Telefoniedienste anfallenden personenbezogenen Daten werden grundsätzlich nicht zu einer Leistungs- und Verhaltenskontrolle verwendet. Die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zur Sicherstellung eines ordnungsgemäßen Betriebs der E-Mail-/Internet-Dienste ist das berechtigte Interesse des Vereins. Die erfassten Protokoll- und Verbindungsdaten werden ausschließlich zum Zweck der Abrechnung der Internet-Nutzung, der Gewährleistung der Systemsicherheit, der Abwehr und/oder Analyse von Cyberkriminalität, der Steuerung der Lastverteilung im Netz und Optimierung des Netzes, der Analyse und Korrektur von technischen Fehlern und Störungen, Missbrauchskontrolle und bei Verdacht auf Straftaten verwendet. Die Verarbeitung der gespeicherten personenbezogenen Daten wird mit Ausnahme der gem. 3.5. von der Archivierung erfassten Daten nach ca. 3 Monaten eingeschränkt, die Daten sind dann nur noch Bestandteil der Langzeitarchivierung.

(3) Aufgrund gesetzlicher Vorgaben, insbesondere nach § 257 Handelsgesetzbuch (HGB) und § 147 Abgabenordnung (AO) ist der Arbeitgeber verpflichtet, über mehrere Jahre geschäftliche Unterlagen und Daten aufzubewahren und zu speichern. Soweit sich unter den geschäftlichen Daten auch private Daten des Arbeitnehmers aufgrund einer etwaigen privaten Nutzung der IT-Systeme, IT-Services und Daten und des Internets befinden, regelt diese Ordnung die Speicherung dieser etwaig anfallenden privaten personenbezogenen Daten.

(4) Bei E-Mails, Textnachrichten, Sprachnachrichten oder anderen elektronischen Mitteilungen ist Vorsicht geboten, da falsche oder unangemessene Aussagen nicht nur zur Haftung des Vereins führen können, sondern auch zur persönlichen Haftung und in manchen Fällen zu strafrechtlicher Haftung. Beschäftigte und Ehrenamtliche müssen immer davon ausgehen, dass ihre E-Mails, SMS, Sprachnachrichten oder andere elektronische Kommunikation von Dritten abgerufen, gelesen oder angehört werden können und dass, unabhängig davon, wie vertraulich oder schädlich dies ist, eine Offenlegung aus Gründen des Datenschutzes, der Informationsfreiheit oder anderer Gesetze, Gerichtsverfahren oder Ermittlungen durch Aufsichtsbehörden erfolgen muss, wenn sie für die untersuchten Fragen relevant sind. Insbesondere bei elektronischer Kommunikation ist die gleiche Sorgfalt anzuwenden wie bei schriftlicher Kommunikation. Mehrdeutigkeit und Ungenauigkeit sollten vermieden werden.

3.7 Missbrauchskontrolle

(1) Alle Beschäftigten und Ehrenamtlichen haben das Recht und die Pflicht, den vermuteten oder tatsächlichen Missbrauch und Missbrauchsversuche der IT-Systeme, IT-Services und Daten dem Verein bzw. ihrem Vorgesetzten mitzuteilen.

(2) Eine personenbezogene Kontrolle der Nutzung der IT-Systeme, IT-Services und Daten findet nur bei konkretem Verdacht eines Verstoßes gegen diese Bestimmungen statt. Der Verein ist insofern berechtigt, zur Klärung des Verdachts eine personenbezogene Kontrolle und Auswertung vorzunehmen, d. h. insbesondere Einsicht in abgespeicherte Daten zu nehmen, den Inhalt den mit dem Verdacht befassten Personenkreis offen zu legen und zu sichern. Die anfallenden Protokolldaten werden nur zur Klärung des konkreten Verdachts ausgewertet.

(3) Bei Feststellungen eines Missbrauchs der IT-Systeme, IT-Services und Daten ist der Verein berechtigt,

a) Zugriffe auf offensichtlich nicht dienstliche und/oder sicherheitsgefährdende Inhalte zu sperren,
b) dem betreffenden Beschäftigten oder Ehrenamtlichen die Nutzungsberechtigung zu entziehen bzw. diese einzuschränken,
c) arbeitsrechtliche Konsequenzen unter Einbeziehung der Stellungnahme der betreffenden Beschäftigten zu prüfen und durchzusetzen.

3.8 Ausscheiden aus dem Verein

Alle geschäftlichen Daten unterliegen den gesetzlichen Aufbewahrungsfristen. Nach dem Ausscheiden eines Beschäftigten oder Ehrenamtlichen werden seine geschäftlichen Daten archiviert und können nötigenfalls zu rechtlichen oder behördlichen Zwecken stichprobenhaft eingesehen werden. Durch seine Verpflichtung auf die Ordnung zum Umgang mit IT-Systemen, IT-Services und Daten bestätigt der Beschäftigte oder Ehrenamtliche sein Einverständnis mit dieser Vorgehensweise.

Alle durch den Verein bereitgestellten Endgeräte (PC, Notebook, Smartphone, Tablet, etc.) sind dem jeweiligen Vorgesetzten, einer durch den jeweiligen Vorgesetzen festgelegten Person oder der IT zurückzugeben.

Die Accounts zu IT-Systemen und IT-Services werden deaktiviert.

4. IT-Verantwortlichkeiten

4.1 Interne und externe IT

Die folgenden Tätigkeiten werden grundsätzlich nur durch die interne oder externe IT wahrgenommen. Dem Beschäftigten sind diese Tätigkeiten nicht gestattet.

(1) Sicherstellung der Verfügbarkeit der lokalen IT-Systeme des Vereins, IT-Services und Daten.
(2) Erstellung der Datensicherung mit allen lokalen Vereinsdaten.
(3) Dauerhafte Überwachung und Pflege des regelmäßigen Backups.
(4) Sicherstellung eines geeigneten Lagerplatzes für die Datensicherung (geschützt vor äußeren Einwirkungen wie Feuer, Wasser, Kälte, Diebstahl).
(5) Betreuung und Konfiguration der lokalen Server und Clientsysteme des Vereins inkl. Update- und Patchmanagement.
(6) Erfassung und Inventarisierung der eingesetzten Client-Hardware des Vereins (PCs, Notebooks, Monitore, externe Speichermedien).
(7) 1st, 2nd und 3rd Level Support.
(8) Abgleich der eingesetzten Client-Betriebssysteme des Vereins mit den vorhandenen Client-Betriebssystemlizenzen und Meldung an die IT bei Unter- oder Überdeckung.
(9) Dokumentation der Zugriffsrechte jedes einzelnen Benutzers auf die jeweiligen lokalen Netzwerkressourcen und die IT-Services.
(10) Sicherstellung der Installation des aktuellen Virenscanners auf den im Netzwerk befindlichen Client-Systemen des Vereins.
(11) Schnellstmögliche Beseitigung bei Auftreten von Schadcode (Malware, Viren, Würmern, Trojaner, etc.) auf Datenverarbeitungsgeräten, die durch den Verein bereitgestellt werden.
(12) Sicherstellung der 24/7-Verfügbarkeit aller zentralen Serversysteme des Vereins in Deutschland.
(13) Dokumentation der Zugriffsrechte aller in Deutschland gehosteten Serversysteme und Netzlaufwerke des Vereins.
(14) Zentralisierte Lizenz-Verwaltung für Software und Services des Vereins.

4.2 Gebrauch privater Endgeräte bei Cloudanwendungen

Für Beschäftigte und Ehrenamtliche gilt: Sofern beim Gebrauch privater Endgeräte die Verarbeitung von Daten des Vereins ausschließlich in Cloudanwendungen (Microsoft Office 365) ohne lokale Synchronisation der Daten des Vereins auf das private Endgerät erfolgt, sind die folgenden Sicherheitsvorkehrungen verpflichtend:

(1) Das private Endgerät (Bsp. PC, Laptop, Notebook, Tablet, Smartphone) ist vor Schadcode (Viren, Trojaner, Würmer, etc.) mithilfe geeigneter Programme (Antivirus, Antispam, Firewall, etc.) zu schützen.
(2) Das Auftreten von Schadcode (Viren, Trojaner, Würmer, etc.) ist unverzüglich der IT per Telefon und E-Mail zu melden.
(3) Das mobile Endgerät (Bsp. Tablet, Smartphone) ist durch eine sichere PIN oder biometrischen Schutz (Fingerabdruck, Face ID, etc.) vor unbefugtem Zugriff zu schützen.

Sofern die Arbeit ausschließlich in Cloudanwendungen (Microsoft Office 365) erfolgt und nur die

Sicherheitsvorkehrungen 1), 2) und 3) eingehalten werden, sind dem User folgende Funktionen untersagt:

(4) Einbinden E-Mail Postfach des Vereins Adresse in private und/oder lokale E-Mail Clients.
(5) Synchronisation von SG Stern Daten auf den PC, Tablet, Smartphone.
(6) Das temporäre Downloaden von SG Stern Daten vom SharePoint und die lokale Bearbeitung.

Eine hybride Variante ist möglich. So kann auf einem privaten PC/Notebook ausschließlich onlinegearbeitet werden, auf dem Smartphone bei Einhaltung aller Sicherheitsvorkehrungen aber dennoch das E-Mail Postfach des Vereins im E-Mail Client eingebunden werden.

4.3 Gebrauch privater Endgeräte bei lokaler Synchronisation

Für Beschäftigte und Ehrenamtliche gilt darüber hinaus: Sofern beim Gebrauch privater Endgeräte die Verarbeitung von Daten mit lokaler Synchronisation der Daten des Vereins auf das private Endgerät erfolgt, sind ergänzend zu den o. g. Maßnahmen die folgenden Sicherheitsvorkehrungen verpflichtend:

(1) Auf dem privaten Endgerät ist ein Betriebssystem zu verwenden, für das Sicherheitsupdates seitens des Herstellers bereitgestellt werden. Betriebssysteme, für die keine Sicherheitsupdates mehr zur Verfügung gestellt werden, dürfen nicht verwendet werden.
(2) Für das Betriebssystem und die verwendete Anwendungssoftware sind Updates und Sicherheitspatches unverzüglich nach Verfügbarkeit zu installieren.
(3) Mobile Datenträger (z. B. Festplatten in Notebooks, externe Festplatten, USB-Sticks, etc.), die personenbezogene Daten beinhalten, sind nur verschlüsselt oder passwortgeschützt zu verwenden. Sollte der Ehrenamtliche feststellen, dass der Datenträger nicht verschlüsselt oder passwortgeschützt ist, so hat er diesen unverzüglich mit einem Passwort zu verschlüsseln. Bei weiteren Fragen wendet er sich umgehend an die IT.
(4) Für die privaten Endgeräte (Bsp. PC, Laptop, Notebook) sind zum Schutz vor unbefugten Zugriffen Passwörter mit folgenden Kriterien zu vergeben: Mindestlänge von zwölf Zeichen, alphanumerisch (Buchstaben (Groß- und Kleinschreibung) und Zahlen) und mit den folgenden Sonderzeichen: # $ & - ! ? % = : ( ). Die letzten 5 Passwörter dürfen dabei nicht wiederverwendet werden.
(5) Zur Verhinderung der Einsicht durch Unbefugte muss die automatische Sperrung bei Inaktivität nach einem angemessenen Zeitraum aktiviert sein. Einzige Ausnahme bilden die vom Verein bereitgestellten iPads zum Streaming von Online-Kursen. Hier kann die Bildschirmsperre deaktiviert werden, um die Übertragung der Live-Kurse nicht zu unterbrechen. Nach Beendigung des Live-Kurses ist das iPad manuell zu sperren (siehe 1.7, Absatz 1).
(6) Ein Rooting oder Jailbreak des privaten Endgerätes darf nicht durchgeführt werden (Veränderung des Betriebssystems zur Erweiterung von Zugriffsrechten).

5. Verstoß gegen die Ordnung zum Umgang mit IT-Systemen, IT-Services und Daten

Diese Ordnung zum Umgang mit IT-Systemen, IT-Services und Daten ist von entscheidender Bedeutung. Werden diese nicht beachtet oder eingehalten, kann dies unter bestimmten Umständen bei Beschäftigten zu schwerwiegenden arbeitsrechtlichen und bei Ehrenamtlichen zu privatrechtlichen Konsequenzen bis hin zur Kündigung bei Beschäftigten und bei Ehrenamtlichen Kündigung der Mitgliedschaft und Entzug der Erlaubnis, ehrenamtlich für den Verein tätig zu sein mit oder ohne vorherige Abmahnung führen.

6. Anhang

6.1 Begriffe und Definitionen, Abkürzungen, technische Fragen

Für Fragen zu Begriffen, Definitionen, Abkürzungen und andere technische Fragen wenden Sie sich bitte an die IT.

6.2 Änderungshistorie

Vers.	**Datum**	**Erstellt**	**Geprüft**	**Freigegeben**	**Beschreibung der Änderung**
1.0	24.02.2020	Schwinge	Croissant, Langer	Langer	Ersetzt bisherige IT-Richtlinie
1.1	04.12.2020	Schwinge	Croissant, Langer	Langer	Format, Aufbau, Rechtschreibung
1.2	23.03.2021	Schwinge	Croissant, Langer	Langer	Format, Aufbau, Rechtschreibung
1.3	16.02.2022	Schwinge	Croissant, Langer	Langer	Zusammenführung der IT-Richtlinien für Haupt- und Ehrenamt; Vereinfachung der Nutzung von Online Diensten unter 4. IT-Verantwortlichkeiten
1.4	23.06.2022	Schwinge	Croissant, Langer	Langer	Vereinfachte Erläuterungen unter 4. IT-Verantwortlichkeiten
1.5	09.08.2023	Schwinge	Handte, Langer	Langer	Format, Rechtschreibung, Änderung in Ordnung und damit einhergehende Regelungen

6.3 Dokumentinformation

Verantwortlicher	Boris Langer, Vorstand Compliance (§26 BGB)
Anwendungsbereich	SG Stern Deutschland e.V. und die SG Stern Berlin e.V.
Zielgruppe	Beschäftigte und extern Tätige der SG Stern Deutschland e.V. und der SG Stern Berlin e.V.

Verteilung	Beschäftigte und extern Tätige der SG Stern Deutschland e.V. und der SG Stern Berlin e.V.
Gültig ab	20.08.2020, die jeweils aktuelle Version des Dokuments ist über den SharePoint zugänglich.