1. Einleitung

Alle kirchlichen Einrichtungen sind für IT-Sicherheit verantwortlich. Informations- und Kommunikationstechnik (IT) ist in heutiger Zeit ein unverzichtbares Instrument zur Erfüllung von Aufgaben kirchlicher Stellen im Bereich der evangelischen Kirchen und ihrer Diakonie. IT-Sicherheit stellt einen Teil der Informationssicherheit dar.

Informationssicherheit sorgt dafür, dass die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit gewahrt werden. **Vertraulichkeit** schützen bedeutet, die IT-Systeme und Anwendungen so zu sichern, dass nur autorisierte Personen auf die verarbeiteten Daten Zugriff haben. **Integrität** schützt die Daten vor Manipulationen. **Verfügbarkeit** hingegen sorgt dafür, dass Daten im gewünschten Zeitraum zur Verfügung stehen und darauf zugegriffen werden kann.

Somit müssen auch die kleinen kirchlichen Einrichtungen Maßnahmen zur Informationssicherheit umsetzen. Dieses Konzeptionskapitel übernimmt größtenteils das von der EKD für kleine kirchliche Einrichtungen empfohlene Muster IT-Sicherheitskonzept. Dieses Dokument muss regelmäßig fortgeschrieben und mit der/dem zuständigen IT-Sicherheitsbeauftragte/-en abgestimmt werden. Es bietet sich an, die Regelungen und die Checkliste quartalsweise oder in kürzeren Intervallen, mindestens aber einmal im Jahr zu überprüfen und ggf. anzupassen. Hierbei muss man sich der Tatsache bewusst sein, dass IT- Sicherheit kein statischer Zustand ist, sondern sich in einem stetigen Prozess fortentwickelt.

Kleine Organisationen werden wie folgt definiert: kleinste und kleine Einrichtungen verfügen über kein geschultes IT-Personal, nur eine minimale Infrastruktur und eine überwiegend dezentrale Datenhaltung, z. T. zentrale Anwendungen (Melde-, Finanz- und Personalwesen). Zudem existiert z. T. keine ausreichende Abgrenzung zu privaten Bereichen (Räume und Geräte). In der Regel gibt es keine IT-Standards (Datensicherung, Kennwortregelungen) und auch keine Server.

Mittlere und große Einrichtungen hingegen verfügen über eigenes geschultes IT-Personal oder externe Mit- arbeitende sowie über eine professionelle IT-Infrastruktur mit eigenen Servern. Zudem existieren in der Regel bereits unterschiedlich ausgeprägte IT-Standards (z. B. Datensicherung, Kennwortregelungen, Protokollierung). Es gibt z. T. Dienstleistungen, die durch Outsourcing betrieben werden.

Vorgaben zur IT-Sicherheit und zum Datenschutz können sich in Teilen überschneiden. An geeigneter Stelle wird auf das Konzeptionskapitel VII.8 Datenschutz verwiesen.

2. Sensibilisierung der Mitarbeitenden

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden. Nur mit informierten und achtsamen Mitarbeitenden können Sicherheitsmaßnahmen wirksam umgesetzt und eventuelle Sicherheitsvorfälle rechtzeitig erkannt werden.

Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, werden Maßnahmen zu dessen Behebung ergriffen. Häufig ist es notwendig, die betroffenen IT-Systeme oder Standorte sofort zu isolieren, um die Auswirkung des Sicherheitsvorfalls einzudämmen. Die Behebung von Sicherheitsvorfällen wird ausführlich dokumentiert.

Die Sensibilisierung zur IT-Sicherheit wird grundsätzlich durch das *Merkblatt über den Datenschutz in der Evangelischen Kirche im Rheinland für ehrenamtlich Tätige / Mitarbeitende* abgedeckt. Zusätzlich wird anhand der im Anhang befindlichen Checkliste und den regelmäßigen Überprüfungen sensibilisiert.

3. Datensicherungskonzept

Computersysteme und Datenträger (z. B. Festplatten, Speicherkarten) können ausfallen oder manipuliert werden. Durch Verlust oder Veränderungen von gespeicherten Daten können mitunter gravierende Schäden verursacht werden. Durch regelmäßige Datensicherungen werden Schäden durch Ausfälle von Datenträgern, Schadsoftware oder Manipulationen an Datenbeständen nicht verhindert, deren Auswirkungen können aber minimiert werden.

Die zu sichernden Daten und Anwendungen (hauptsächlich dezentral) sind aufgelistet und jeweils einem Verantwortlichen zugordnet.

Backup-Datenträger müssen einerseits im Bedarfsfall schnell verfügbar sein, andererseits sollten sie räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden. Somit sind sie auch bei Notlagen, wie z. B. Brand oder Hochwasser verfügbar.

4. Schutz vor Schadprogrammen

Wenn IT-Systeme mit Schadsoftware (Viren, Würmer, Trojanische Pferde usw.) befallen werden, kann dies die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und der darauf gespeicherten Daten gefährden.

Auf jedem IT-System (z. B. PC, Laptop) muss ein Viren-Schutzprogramm installiert sein. Automatische Updates müssen aktiviert sein. Durch regelmäßige Sicherheitsupdates für Android oder iOS wird sichergestellt, dass auch die mobilen Endgeräte ausreichend geschützt sind.

Infizierte IT-Systeme müssen unverzüglich von allen Datennetzen getrennt und dürfen bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden.

Auf allen IT-Systemen müssen für die Betriebssysteme sowie für alle installierten Treiber und Programme zeitnah die jeweils hierfür veröffentlichten sicherheitsrelevanten Updates und Patches eingespielt werden. Dies gilt besonders für Programme, mit denen auf Fremdnetze zugegriffen wird (z. B. Webbrowser).

5. Regelungen für Hard- und Software

Für den sicheren Einsatz von IT-Systemen und IT-Anwendungen ist es erforderlich, dass Abläufe und Vorgänge, die diese IT-Systeme berühren, so gestaltet werden, dass das angestrebte Niveau der Informationssicherheit erreicht bzw. beibehalten wird.

Alle Mitarbeitenden sind darüber informiert, dass nur explizit von der Einrichtung freigegebene und korrekt lizensierte Standardsoftware eingesetzt werden darf.

Es wird nur solche Software eingesetzt, für die noch regelmäßig Sicherheitsupdates und -patches ausgeliefert werden.

Durch eine geeignete Benutzerkonten- und Rechteverwaltung ist sichergestellt, dass nur diejenigen Personen Zugriff auf IT-Systeme, Applikationen und Informationen haben, die aufgrund ihrer Aufgaben dazu berechtigt sind.

Bei der normalen Nutzung der Clients wird nicht mit administrativen Rechten (Admin-Benutzer) gearbeitet. Dies ist nur zu administrativen Tätigkeiten zulässig, die unbedingt von normalen Aufgaben getrennt durchzuführen sind.

Um sicherzustellen, dass nur Befugte auf Systeme und Informationen zugreifen können, ist eine benutzerspezifische Anmeldung mit Passwort und ggfs. weiteren Prüfungen (z. B. Zwei-Faktor-Authentifizierung) etabliert. Die Benutzer sind über die dafür notwendigen Regelungen und deren Anwendung sowie deren Hintergründe explizit informiert.

Das Passwort bei IT-Systemen besteht aus mindestens 8 Zeichen. Es setzt sich aus Klein- und Großbuchstaben, sowie aus Zahlen oder Sonderzeichen zusammen.

Bei der Beendigung von Arbeits- oder Ehrenamtsverhältnissen ist die geordnete Über- und Rückgabe der Geräte und Daten sicherzustellen.

Das sichere Löschen und Vernichten von Daten auf Datenträgern (z.B. Server, Clients, Netzkomponenten, Smartphones) wird vor der Aussonderung oder vor einer Weitergabe der Datenträger und Geräte vorgenommen.

6. Büroraum / Lokaler Arbeitsplatz

Der Büroraum ist ein Raum, in dem sich eine oder mehrere Personen aufhalten, um dort der Erledigung ihrer Aufgaben nachzugehen. Diese Aufgaben können (auch IT-unterstützt) aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.

Fenster und Türen werden verschlossen, wenn ein Raum nicht besetzt ist. Büroräume sind so ausgestattet, dass schutzbedürftige Datenträger und Dokumente weggeschlossen werden können. Dazu sind beispielsweise verschließbare Schreibtische, Rollcontainer oder Schränke vorhanden.

Allen Mitarbeitenden ist bewusst, dass auch in Büroräumen die vorhandenen IT- Geräte, Zubehör, Software oder Daten ausreichend gegen Diebstahl, Zerstörung und Veränderungen geschützt werden müssen.

In Büros mit Publikumsverkehr sind Diebstahlsicherungen zum Schutz von IT-Systemen (z. B. Laptops) eingesetzt, da andernfalls die Gefahr besteht, dass solche Geräte in einem unbewachten Augenblick abhandenkommen.

7. Mobiler Arbeitsplatz

Ein mobiler Arbeitsplatz kann auch z. B. von Telearbeitern, freien Mitarbeitern oder Selbstständigen sowie von Ehrenamtlichen genutzt werden. Bei einem mobilen Arbeitsplatz kann die infrastrukturelle Sicherheit nicht so vorausgesetzt werden, wie sie in einer Büroumgebung innerhalb der Räumlichkeiten einer Institution anzutreffen ist.

Dienstliche Aufgaben werden häufig auch an wechselnden Arbeitsplätzen und in unterschiedlichen Umgebungen durchgeführt. Die dabei verarbeiteten Informationen sind angemessen geschützt (z. B. durch Sperren des Bildschirms oder Anbringen eines Sichtschutzes).

Die Leistungsfähigkeit von mobilen IT-Systemen wie beispielsweise Laptops, Smartphones und Tablets wächst ständig und lässt es zu, große Mengen geschäftsrelevanter Informationen außerhalb der Räume der jeweiligen Institution zu bearbeiten. Dabei ist zu beachten, dass meist die infrastrukturelle Sicherheit nicht der einer Büroumgebung entspricht.

An mobilen Arbeitsplätzen bleiben weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt. Sie sind zumindest gegen einfache Wegnahme gesichert, z. B. mit einer Diebstahlsicherung oder in Schränke eingeschlossen.

Beim Einsatz mobiler Geräte sind die Festplatten der Rechner grundsätzlich immer verschlüsselt.

8. Arbeitsplatz-Rechner

Als Arbeitsplatz-Rechner wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt.

Eine Bildschirmsperre ist eingerichtet, die sich sowohl manuell vom Benutzer aktivieren lässt als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch aktiviert wird.

Alle Mitarbeitenden sind dazu zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT- Anwendung abzumelden.

E-Mails werden verschlüsselt von und zu Mail-Servern übertragen werden (z. B. mittels SSL/TLS).

Ein Laptop oder Notebook ist ein IT-System mit einer transportfreundlichen, kompakten Bauform, welches aufgrund dieser mobil genutzt werden kann. Ein Laptop ist ein vollwertiger Arbeitsplatz-Rechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden.

Bei diesen Geräten sind die Festplatten grundsätzlich zu verschlüsseln.

Zugriffe von einem Laptop von außerhalb auf das interne Netz sind abgesichert (über SSL/TLS oder VPN verschlüsselt).

9. Mobiltelefon / Smartphone

Mobiltelefone bzw. Smartphones sind inzwischen alltäglicher Bestandteil der kirchlichen Kommunikationsinfrastruktur geworden. Neben herkömmlichen Telefongesprächen bieten die Geräte meist noch eine Vielzahl an zusätzlichen Funktionen wie das Verschicken von SMS, MMS, E-Mails, die Nutzung des Internets über WLAN oder Mobilfunk. Zudem existieren auch Apps, wie z. B. Whatsapp oder Threema, die Funktionalitäten zur Datenübertragung ermöglichen.

Verlorene Geräte müssen über den Mobilfunkanbieter umgehend gesperrt werden.

Die Sicherheitsmechanismen von Mobiltelefonen (z. B. Eingabe einer PIN oder eines Passworts, Fingerabdruck, etc.) sind bei dienstlichen Geräten aktiviert.

Vertrauliche Daten, wie personenbezogene Daten oder Zugangsdaten zum Netz der Institution, werden auf den Geräten vermieden. Eine unumgängliche Speicherung auf dem Gerät (inklusive Speicherkarte) erfolgt ausschließlich in verschlüsselter Form. Das Senden von vertraulichen Daten ist nur über gesicherte, von der kirchlichen Organisation bereitgestellte Transportwege erlaubt (insb. EKiR-Portal mit E-Mail- und Cloud-Service). Nicht dazu gehören z. B. Skype, Whatsapp oder private E-Mail (vgl. Konzeptionskapitel VIII.8 Datenschutz).

10. Netzwerke

Netzwerke sind für die Informationsübertragung unerlässlich. Dies umfasst lokale Netzwerke, um z. B. einen Drucker anzusteuern, oder das Nutzen entfernter Dienste über das Internet. Netzwerke sind nach den Nutzenden und den damit verbundenen Schutzbedarfen mindestens durch VLANs separiert, z. B. ein Netzwerk für Mitarbeitende mit Arbeitsplatzrechnern und ein anderes Netzwerk für Gruppen oder weitere Gäste. Ein Austausch zwischen den Netzwerken erfolgt nur nach definierten Ausnahmen.

Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netze aufzubauen oder bestehende drahtgebundene Netze zu erweitern. WLANs können aufgrund der einfachen Installation nicht nur dauerhaft, sondern auch für temporär zu installierende Netze, wie z. B. für Veranstaltungen, verwendet werden.

Die Kommunikation im WLAN folgt mindestens dem Verschlüsselungsstandards WPA2. Die Netzwerkseparierung wird auch bei WLAN-Netzen angewendet.

Die kryptographischen Schlüssel für den Zugriff auf ein WLAN sind zufällig generiert und werden regelmäßig geändert. Voreingestellte Standardpasswörter sind vor Inbetriebnahme unbedingt zu wechseln.

Bei der Aussonderung von WLAN-Komponenten werden die Authentifizierungsinformationen für den Zugang zum WLAN und andere erreichbare Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert. Hierzu ist die Komponente auf die Werkseinstellung zurückzusetzen.

11. Mobile Datenträger

Mobile Datenträger werden für eine Vielzahl von Zwecken eingesetzt, beispielsweise für den Datentransport, die Speicherung von Daten oder die mobile Datennutzung. Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern. Hierzu gehören unter anderem Disketten, externe Festplatten, CD-ROMs, DVDs, Magnetbänder und USB-Sticks.

Die Mitarbeitenden sind über die Risiken in Hinblick auf mobile Datenträger und über die erforderlichen Sicherheitsmaßnahmen informiert.

Aufgrund des erhöhten Schutzbedarfs ist der Austausch von vertraulichen Daten über mobile Datenträger nicht gestattet (vgl. Konzeptionskapitel VIII.8 Datenschutz).

12. Internetnutzung

Das Internet als wichtiges Informations- und Kommunikationsmedium ist aus dem Arbeitsalltag nicht mehr wegzudenken. In den meisten Organisationen ist die Nutzung von E-Mail, Informationsangeboten, Internet- Dienstleistungen, Online-Banking und Online-Shopping selbstverständlich. Gleichzeitig muss verhindert werden, dass durch die Anbindung der eigenen Geräte an das Internet für die Organisation nicht akzeptable Risiken entstehen.

Alle Mitarbeitenden sind über das Potential, aber auch die Risiken der Internet-Nutzung informiert. Sie wissen, welche Rahmenbedingungen bei der Nutzung von Internet-Diensten zu beachten sind. Dazu gehört insbesondere, dass sie die Regeln kennen, um Dienste sicher zu nutzen und sich korrekt im Internet zu verhalten, beispielsweise in (Web-)Blogs oder sozialen Netzwerken (z. B. Instagram, Facebook, X), vgl. Konzeptionskapitel VIII.17 Social Media Guideline.

Bei vielen Internet-Diensten müssen sich die Benutzer mittels Benutzernamen und Passwort authentisieren. Dabei werden die allgemeinen Regeln zur sicheren Verwendung von Passwörtern (siehe Hard- und Software) eingehalten. Wichtig ist insbesondere, dass die Passwörter nicht leicht zu erraten sind. Für verschiedene Internet-Dienste werden verschiedene Passwörter verwendet. Vor allem werden dafür keine Passwörter genutzt, die für IT-Systeme oder IT-Anwendungen innerhalb der kirchlichen und diakonischen Einrichtungen verwendet werden.

13. Checkliste für kleine Organisationen

Nummer	Frage	Referenz	Umgesetzt
1.	Werden neue Mitarbeitende und ehrenamtlich Tätige bei der Einstellung auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen?	Kap. 1	
2.	Sind die wichtigen Schlüsselpositionen durch einen Vertreter besetzt?	Kap. 1	
3.	Haben alle Mitarbeitenden und ehrenamtlich Tätigen eine Verpflichtung zur Wahrung des Datengeheimnisses unterschrieben?	Kap. 2	
4.	Gibt es eine Übersicht über relevante Datenarten und deren Schutzbedarf bzw. die getroffenen Sicherungsmaßnahmen?	Kap. 3	
5.	Werden Backup-Datenträger in einem gesonderten Raum aufbewahrt?	Kap. 3	
6.	Sind auf allen Clients Virenschutzprogramme installiert?	Kap. 4	
7.	Werden Betriebssysteme und Anwendungen regelmäßig aktualisiert?	Kap. 4	
8.	Wird ein Verzeichnis aller organisationseigenen IT-Geräte geführt und wurde dieses innerhalb des letzten Jahres aktualisiert?	Kap. 5	
9.	Gibt es eine Checkliste für Mitarbeitende zur Beendigung des Arbeitsverhältnisses bzw. für Ehrenamtliche zur Beendigung ihrer Tätigkeit?	Kap. 5	
10.	Gibt es eine Benutzer- und Rechteverwaltung für IT-Systeme und An-wendungen?	Kap. 5	
11.	Gibt es Passwortregelungen für IT-Systeme und Anwendungen und werden diese umgesetzt?	Kap. 5	
12.	Werden alle Mitarbeitenden über die Regelungen zur Nutzung von Standardsoftware informiert?	Kap. 5	
13.	Wird ausschließlich Software aus vertrauenswürdigen Quellen installiert?	Kap. 5	
14.	Gibt es regelmäßige Kontrollen bezüglich der installierten Software?	Kap. 5	
15.	Sind auf Clients und Servern automatische Updates aktiviert?	Kap. 5	
16.	Gibt es spezielle Handlungsanweisungen und Tools zum Löschen und Vernichten von Daten?	Kap. 5	
17.	Sind Türen und Fenster in der Regel verschlossen, wenn die Mitarbeitenden nicht am Platz sind?	Kap. 6	
18.	Sind in den Büros verschließbare Schreibtische oder Schränke vorhanden?	Kap. 6	
19.	Gibt es in Büros mit Publikumsverkehr Diebstahlsicherungen für IT-Systeme?	Kap. 6	
20.	Sind am mobilen Arbeitsplatz verschließbare Schreibtische oder Schränke vorhanden?	Kap. 7	
21.	Gibt es Regelungen, welche dienstlichen Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der	Kap. 7	

	Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen?		
22.	Ist auf allen Clients die Bildschirmsperre aktiviert?	Kap. 8	
23.	Ist der Zugriff von mobilen Laptops auf das LAN per VPN abgesichert?	Kap. 8	
24.	Ist die Verschlüsselung von E-Mail-Kommunikation zwischen Client und Server aktiviert?	Kap. 8	
25.	Ist bei allen Mobiltelefonen/Smartphones die Eingabe der Geräte-PIN aktiviert?	Kap. 9	
26.	Werden alle vertraulichen Daten nur verschlüsselt auf Mobiltelefonen/Smartphones oder Speicherkarten gespeichert?	Kap. 9	
27.	Wird bei WLAN das Verschlüsselungsverfahren WPA2 eingesetzt?	Kap. 10	
28.	Werden die Schlüssel für den WLAN-Zugriff regelmäßig gewechselt?	Kap. 10	