ANLAGE 1: ANFORDERUNGEN FÜR PRAXEN

SOFTWARE: RECHNER-PROGRAMME, MOBILE APPS UND INTERNET-ANWENDUNGEN

NR	ZIELOBJEKT	ANFORDERUNG	ERLÄUTERUNG	GELTUNG AB	WEITERE HINWEISE ETC.
1.	Mobile Anwendungen (Apps)	Sichere Apps nutzen	Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps restlos löschen	01.04.2021	– für IOS: "App Store" – für Android: "Google Play" verwenden und in den Sicherheitseinstellungen keine Apps aus externen Quellen zulassen.
2.	Mobile Anwendungen (Apps)	Aktuelle App-Versionen	Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.	01.04.2021	– Autoupdates aktivieren
3.	Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.	01.01.2022	– Verschlüsselung von Android (PIN oder Passwort einrichten)/ IOS ("Code-Sperre") aktivieren.
4.	Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Keine vertraulichen Daten über Apps versenden.	01.04.2021	– Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzerprofile erstellt werden, muss der Datenversand entsprechend eingeschränkt werden. – Vor der App-Benutzung sollte überprüft werden, ob eine App ungeschützte Protokollierungs- oder Hilfsdateien schreibt, die vertrauliche Informationen enthalten.
5.	Office-Produkte	Verzicht auf Cloud-Speicherung	Keine Nutzung der in Office-Produkte integrierte Cloud-Speicher zur Speicherung personenbezogener Informationen	01.04.2021	– Kein Microsoft 365 (ehemals Office 365), OneDrive verwenden. – vgl. Anlage 1 - Anforderung Nr. 16
6.	Office-Produkte	Beseitigung von Rest-Informationen vor Weitergabe von Dokumenten	Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.	01.04.2021	– Entfernen der Metadaten wie "Autor(en)", zuletzt "geändert von" der Dokumente unter → Datei -> Eigenschaften.
7.	Internet-Anwendungen	Authentisierung bei Webanwendungen	Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.	01.04.2021	– Achten sie auf sichere 2 Faktor Authentisierung oder – verwenden sie hinreichend komplexe Passwörter (vgl. Anlage 1 - Anforderung Nr. 34) oder Passwortmanager mit generierten Passwörtern. – Achten Sie auf verschlüsselte Verbindungen vgl. Anlage 1 - Anforderung Nr. 10
8.	Internet-Anwendungen	Schutz vertraulicher Daten	Stellen Sie ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.	01.04.2021	– Chrome, Firefox, Edge mittels "Strg" + "Umschalt" + "Entf": Löschen der Browserdaten – Safari: "cmd" + "alt" + "E" Löschen der Browserdaten. – oder Browser wie "Firefox Klar" verwenden, die diese Daten mit einem Klick oder nach Beendigung der Anwendung automatisch löschen.
9.	Internet-Anwendungen	Firewall benutzen	Verwendung und regelmäßiges Update einer Web App Firewall.	01.01.2022	– Eine Web Application Firewall ist eine Spezialform einer Application Firewall für das HTTP-Protokoll, um die damit verbundeneren Angriffe zu minimieren. – Bei der Bereitstellung einer web-Anwendung sollten sie entweder eine open source Lösungen (wie ModSecurity, Waf2Py oder OctopusWAF) oder eine spezielle kommerzielle Appliance verwenden. Zu dem Einsatz einer Web Application Firewall gehört auch die richtige Konfiguration der Firewall, ggf. die Härtung der zugrunde liegenden Hardware und des Betriebssystems und die regelmäßige Wartung und Updates
10.	Internet-Anwendungen	Kryptografische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.	01.04.2021	– Auf https achten, Plug-In/ Erweiterung wie HTTPS Everywhere verwenden – Beispielsweise statt http://www.kbv.de besser https://www.kbv.de verwenden. – Dies wird durch ein "Schloss" als Icon im Webbrowser visualisiert. Durch anklicken des Schlosses lasen sich die Informationen zu dem Zertifikat und dem Herausgeber des Zertifikats einsehen.
11.	Internet-Anwendungen	Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.	01.01.2022	– Mittels des sogenannten "Captcha-Mechanismus" lassen sich automatisierte Zugriffe begrenzen. – Durch zeitlich verzögerte Anmeldeversuche bei Falscheingaben lassen sich missbräuchliche Anmeldeversuche erschweren.

JETZT KOMMENTIEREN

HARDWARE: ENDGERÄTE UND IT-SYSTEME

NR	ZIELOBJEKT	ANFORDERUNG	ERLÄUTERUNG	GELTUNG AB	WEITERE HINWEISE ETC.
12.	Endgeräte	Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras	Mikrofon und Kamera am Rechner sollten grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.	01.04.2021	– Bei der Anschaffung neuer Geräte sollte darauf geachtet werden, dass die Kamera abgedeckt und das Mikrofon ausgeschaltet werden kann, Eine Diode weist meist auf die für aktive Benutzung der Geräte hin, und bietet einen Indikator für missbräuchliche Nutzung.
13.	Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder Abmelden.	01.04.2021	– z.B. 'Windows' + 'L' für Windows – oder 'logout' für Linux
14.	Endgeräte	Regelmäßige Datensicherung	Sichern Sie regelmäßig Ihre Daten.	01.01.2022	– Schützen Sie Ihre Daten durch ein Backup vor Ausfällen von Hard- und Software sowie Verschlüsselungstrojaner. – Erstellen Sie eine Plan der festlegt, welche Daten wie oft gesichert werden sollen. Kombinieren Sie dabei vollständige Backups und inkrementelle Backups. – Prüfen Sie regelmäßig, ob sich die Backups fehlerlos wieder zurückspielen lassen. – Mittels Virtualisierungssoftware lassen sich Abbilder der Rechner erstellen. – Schützen Sie auch Ihre Backups vor Verlust und ungewolltes überschreiben. – Prüfen sie, ob sie die 3-2-1-Regel (3 Kopien auf 2 unterschiedlichen Medien, davon 1 außer Haus) anwenden möchten.
15.	Endgeräte	Einsatz von Viren-Schutzprogrammen	Setzen Sie aktuelle Virenschutzprogramme ein.	01.04.2021	– Verwenden sie "Windows Defender" oder ein kommerzielles Virenschutzprogramme. – Konfigurieren sie welche Daten wann gescannt werden sollen (z. B. alle Dateien vor dem Schreiben, eingehende E-Mail, etc.).
16.	Endgeräte mit dem Betriebssystem Windows	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.	01.01.2022	– vgl. Anlage 1 - Anforderung Nr. 5 – Deinstallieren Sie "OneDrive". Dazu klicken Sie auf den Windowsbutton, dann auf Einstellungen. Klicken Sie in dem geöffneten Fenster auf "Apps", in der angezeigten App-Liste auf "OneDrive" und deinstallieren Sie die App über den Button "deinstallieren".
17.	Endgeräte mit dem Betriebssystem Windows	Datei- und Freigabeberechtigungen	Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.	01.01.2022	– Regeln Sie die Berechtigungen nach dem Need-to-know-Prinzip. D. h. Jede Person sollte nur so viel Berechtigungen, wie zur Bewältigung der Aufgaben nötig sind, auf Programm-, Datei und Verzeichnisebene erhalten. – Mittels Gruppen und Rollen lassen sich Berechtigungen für mehrere Personen für Netzfreigaben einrichten.
18.	Endgeräte mit dem Betriebssystem Windows	Datensparsamkeit	Verwenden Sie so wenige persönliche Daten wie möglich.	01.01.2022	– Jede Verwendung von personenbezogenen Daten muss begründet (Zweckbindung) und in einem "Verzeichnis von Verarbeitungstätigkeiten" nach Artikel 30 DSGVO dokumentiert werden. Dies schließt auch die einzuhaltenden Löschfristen mit ein. Ein Beispiel für solch ein Verzeichnis und eine Ausfüllhilfe dazu gibt es auf den Seiten der KBV unter https://www.kbv.de/html/datensicherheit.php
19.	Smartphone und Tablet	Schutz vor Phishing und Schadprogrammen im Browser	Nutzen Sie aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser.	01.04.2021	– Alle (mobilen) Endgeräte sollten vor Schadprogrammen geschützt werden. Im verwendeten Browser sollte die Funktion „Safe Browsing" bzw. die Funktion zur Warnung vor schädlichen Inhalten aktiviert werden. – vgl. Anlage 1 - Anforderung Nr. 8 – Seien Sie achtsam bei der Eingabe von Zugangsdaten. Überprüfen sie die URL, Seriöse Anbieter verschicken keine E-Mails inklusive einem Link mit der Aufforderung die Zugangsdaten dort einzugeben. Falls sie dazu aufgefordert werden besuchen sie die ihnen bekannten Seiten (z. B. über Bookmarks).
20.	Smartphone und Tablet	Verwendung der SIM-Karten-PIN	SIM-Karten durch PIN schützen. Super-PIN/PUK nur durch Verantwortliche anzuwenden.	01.04.2021	– Die Nutzung der SIM-Karte der Institution sollte durch eine PIN geschützt werden. Die Super-PIN/PUK sollte nur im Rahmen der definierten Prozesse von den Verantwortlichen benutzt werden.
21.	Smartphone und Tablet	Sichere Grundkonfiguration für mobile Geräte	Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräte das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss.	01.01.2022	– Alle mobilen Endgeräte müssen so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen. Dafür muss eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen sollten deaktiviert werden. – Die Freischaltung von Kommunikationsschnittstellen muss geregelt und auf das dienstlich notwendige Maß reduziert werden. Nicht benutzte Schnittstellen sollten deaktiviert werden. – Überprüfen sie regelhaft die Datenschutzeinstellungen der Anwendungen (Apps). Wenn sie sich unsicher sind verweigern sie sämtliche Zugriffe.
22.	Smartphone und Tablet	Verwendung eines Zugriffschutzes	Schützen Sie Ihre Geräte mit einem komplexen Gerätesperrcode.	01.04.2021	– Smartphones und Tablets müssen mit einem angemessen komplexen Gerätesperrcode geschützt werden. – Die Nutzung der Bildschirmsperre muss vorgeschrieben werden. – Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm muss deaktiviert sein. – Alle mobilen Geräte müssen nach einer angemessen kurzen Zeitspanne selbsttätig die Bildschirmsperre aktivieren. – Nach mehreren fehlgeschlagenen Versuchen, den Bildschirm zu entsperren, sollte sich das mobile Gerät in den Werkszustand zurücksetzen. Es sollten dabei die Daten oder die Verschlüsselungsschlüssel sicher vernichtet werden.
23.	Smartphone und Tablet	Updates von Betriebssystem und Apps	Updates des Betriebssystems und der eingesetzten Apps bei Hinweis auf neue Versionen immer zeitnah installieren, um Schwachstellen zu vermeiden. Legen Sie zusätzlich einen festen Turnus (z.B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.	01.04.2021	vgl. Anlage 1 - Anforderung Nr. 2
24.	Smartphone und Tablet	Datenschutz-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen Ihrer Geräte sollten Sie in den Einstellungen restriktiv auf das Notwendigste einschränken.	01.01.2022	– Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen muss angemessen eingeschränkt werden. – Die Datenschutzeinstellungen müssen so restriktiv wie möglich konfiguriert werden. Insbesondere der Zugriff auf Kamera, Mikrofon sowie Ortungs- und Gesundheitsdaten muss auf Konformität mit den organisationsinternen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. deaktiviert werden.
25.	Mobiltelefon	Sperrmaßnahmen bei Verlust eines Mobiltelefons	Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Hinterlegen Sie die dafür notwendigen Mobilfunkanbieter-Informationen, um sie bei Bedarf im Zugriff zu haben.	01.01.2022	
26.	Mobiltelefon	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.	01.01.2022	– Die verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen konfiguriert und genutzt werden. – Die SIM-Karte sollte durch eine sichere PIN geschützt werden. – Das Mobiltelefon sollte durch einen Geräte-Code geschützt werden. – Falls möglich, sollte das Gerät an die SIM-Karte gebunden werden (SIM-Lock). – Die Benutzer sollten über diese Sicherheitsmechanismen informiert werden.
27.	Mobiltelefon	Updates von Mobiltelefonen	Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt.	01.04.2021	– vgl. Anlage 1 - Anforderung Nr. 2 und Nr. 23 – Ein Backup hilft ihnen bei einem fehlgeschlagenen Update. – Überprüfen sie, ob nach den Updates ungewünschte Einstellungen wie die automatisierte Nutzung von Cloud-Speichern aktiviert wurden.
28.	Wechseldatenträger / Speichermedien	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.	01.01.2022	– Mittels Antiviren- bzw. Anti-Malware-Programmen lassen sich Wechseldatenträger vor der Verwendung auf Schadsoftware prüfen.
29.	Wechseldatenträger / Speichermedien	Angemessene Kennzeichnung der Datenträger beim Versand	Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.	01.04.2021	– Entweder sollte der Sender eine Liste führen, die eine Kennzeichnung eines Datenträgers eindeutig zuordenbar macht, oder Sender und Empfänger einigen sich auf eine Systematik, die die Kennzeichnung der Datenträger für beide zuordenbar macht aber keine Rückschlüsse für andere ermöglicht. Z.B. Datenträger: "dd2bbeab-d901-4043-b543-0ce74ce57aae" statt "onkologischer Befund Patient XY".
30.	Wechseldatenträger / Speichermedien	Sichere Versandart und Verpackung	Versand-Anbieter mit sicherem Nachweis-System, Manipulationssichere Versandart und Verpackung.	01.04.2021	– Über die Angebote der sicheren Nachweissysteme wie Einschreiben und Wertsendungen informiert sie ihr Postunternehmen.
31.	Wechseldatenträger / Speichermedien	Sicheres Löschen der Datenträger vor und nach der Verwendung	Datenträger nach Verwendung immer sicher und vollständig Löschen. Ihr Rechner bietet dafür verschiedene Möglichkeiten.	01.01.2022	– Bevor wieder beschreibbare Datenträger weitergegeben, wiederverwendet oder ausgesondert werden, sollten sie in geeigneter Weise gelöscht (mit spezieller Software mehrmals mit Zufallswerten überschrieben) werden. Diese Funktionalität bieten verschieden kommerzielle Anti-Viren und spezielle open Source Programme an.
32.	Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.	01.04.2021	– Es wird empfohlen eine Hardware-Firewall einzusetzen und diese nach den eigenen Anforderungen zu konfigurieren und zu warten. Mindestens sollte dabei Folgendes eingestellt werden: – Nur erlaubte Kommunikationsziele (IP-Adressen und Ports) zulassen (eingehend und ausgehend). – Nur erlaubte Kommunikationsprotokolle zulassen.
33.	Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.	01.04.2021	– Dokumentation der logischen Struktur des Netzes insbesondere Subnetze und wie das Netz zoniert und segmentiert wird. – Änderungen im Netzwerk sollten dokumentiert werden.
34.	Netzwerksicherheit	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.	01.01.2022	– Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden. – Alle Default-Passwörter müssen auf den Netzkomponenten geändert werden. – Die neuen Passwörter müssen ausreichend stark sein. Es sollten mind. 3 verschiedene Zeichenarten verwendet werden (z. B. Buchstaben, Zahlen und Sonderzeichen). Die Länge eines Passworts sollte mind. 12 Zeichen betragen.

JETZT KOMMENTIEREN

Ein Service der Kassenärztlichen Bundesvereinigung (KBV)
Dezernat Digitalisierung und IT

Ansprechpartner

Telefon: 030 40 05 - 21 21
E-Mail: servicedesk@kbv.de

Weitere Informationen

Nutzungsbedingungen
Datenschutz
Impressum