

A1-01 Geregelte Einarbeitung neuer Mitarbeitender			
Neue Mitarbeitende in IT- und Datenschutzregeln einweisen			
Praxis:	Einarbeitung durchführen	Dokument:	Einarbeitungsprotokoll A1-01
IT:		Nachweis:	Unterschrift Mitarbeitende
<i>Neue Mitarbeitende müssen zu Beginn klar erklärt bekommen, welche Aufgaben sie haben, welche Regeln in der Praxis gelten und wie sie richtig arbeiten sollen.</i>			

A1-02 Geregelte Verfahrensweise beim Weggang von Mitarbeitenden			
Beim Ausscheiden alle Zugänge sperren und Geräte zurücknehmen			
Praxis:	Rückgabe prüfen	Dokument:	Offboarding-Formular A1-02
IT:	Zugänge deaktivieren	Nachweis:	Offboarding-Protokoll
<i>Wenn Mitarbeitende die Praxis verlassen, müssen sie alle Unterlagen, Schlüssel, Geräte und Ausweise zurückgeben. Alle Passwörter und Zugänge, die sie kannten, müssen geändert oder gelöscht werden. Sie müssen außerdem daran erinnert werden, dass ihre Schweigepflicht weiter gilt.</i>			

A1-03 Festlegung von Regelungen für den Einsatz von Fremdpersonal			
Regeln für Fremdpersonal festlegen			
Praxis:	Regel erstellen und kommunizieren	Dokument:	Fremdpersonal-Regel A1-03
IT:		Nachweis:	Unterschrift Kenntnisnahme
<i>Externe Personen müssen sich an die gleichen Regeln halten wie das Praxispersonal. Wenn sie nur kurz da sind, müssen sie in sicherheitsrelevanten Bereichen beaufsichtigt werden. Ihre Zugänge dürfen nur so weit wie unbedingt nötig erlaubt werden.</i>			

A1-04 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal			
Vertraulichkeitsvereinbarung vor Zugriff auf Patientendaten			
Praxis:	Vereinbarung unterschreiben lassen	Dokument:	NDA-Vorlage A1-04
IT:		Nachweis:	Unterschiedene Vereinbarung
<i>Bevor externe Personen Zugang zu sensiblen Informationen erhalten, muss mit ihnen schriftlich vereinbart werden, dass sie diese vertraulich behandeln.</i>			
A1-05 Aufgaben und Zuständigkeiten von Mitarbeitenden			
Rollen und Zuständigkeiten dokumentieren			
Praxis:	Rollenliste erstellen	Dokument:	Rollenmatrix
IT:		Nachweis:	Aktuelle Rollenliste
<i>Alle Mitarbeitenden müssen wissen, welche Gesetze und internen Regeln sie einhalten müssen. Ihre Aufgaben, Zuständigkeiten und Zugriffsrechte müssen dokumentiert sein. Sie müssen wissen, dass alle Informationen aus der Arbeit nur für die Praxis bestimmt sind.</i>			
A1-06 Qualifikation des Personals			
Regelmäßig Schulungen/Weiterbildung zu sicherem Arbeiten mit Praxis-IT durchführen			
Praxis:	Schulungsplan (Turnus) festlegen, Teilnahme dokumentieren	Dokument:	Schulungsplan + Teilnahme-Liste A1-06
IT:	Bei Bedarf: Schulungsinhalte und Unterstützung bereitstellen	Nachweis:	Schulungsplan + Teilnahmelisten
<i>Mitarbeitende müssen regelmäßig geschult werden, besonders im Umgang mit der eingesetzten Technik. Es muss sichergestellt sein, dass ihr Wissen aktuell bleibt und sie sich weiterbilden können.</i>			

A1-07 Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden			
Vertrauenswürdigkeit neuer Mitarbeitender prüfen			
Praxis:	Einstellungsscheck durchführen	Dokument:	Checkliste Einstellung A1-07
IT:		Nachweis:	Abgehakte Checkliste
<i>Bei Neueinstellungen sollte geprüft werden, ob Bewerbende vertrauenswürdig sind, zum Beispiel durch das Prüfen von Arbeitszeugnissen und Angaben im Lebenslauf.</i>			
A1-08 Sensibilisierung der Praxisleitung für Informationssicherheit			
Praxisleitung zu Sicherheitsfragen sensibilisieren			
Praxis:	Kurzbriefing durchführen	Dokument:	Agenda/Notiz
IT:		Nachweis:	Protokoll
<i>Die Praxisleitung muss verstehen, wie wichtig Informationssicherheit ist, und Schulungen und Sicherheitsmaßnahmen aktiv unterstützen.</i>			
A1-09 Einweisung des Personals in den sicheren Umgang mit IT			
Sicheren Umgang mit PCs, Passwörtern, Druckern erklären			
Praxis:	Einweisung Team	Dokument:	1-Seiter Anleitung
IT:		Nachweis:	Unterschriftenliste
<i>Alle Mitarbeitenden und externen Nutzenden müssen erklärt bekommen, wie sie Computer, Programme und Geräte sicher benutzen.</i>			

A1-10 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit			
Schulung zu Phishing und E-Mail-Gefahren durchführen			
Praxis:	Schulung durchführen	Dokument:	Schulungsfolien
IT:		Nachweis:	Teilnahmeliste
<i>Mitarbeitende sollen je nach Aufgabe regelmäßig zu Themen der Informationssicherheit geschult werden.</i>			
A1-11 Absicherung der Netzübergangspunkte			
Internetanschluss technisch absichern			
Praxis:	IT-Termin beauftragen, Konfigurationsnachweis ablegen	Dokument:	IT-Termin
IT:	Schutz am Internetanschluss einrichten; nur notwendige Verbindungen erlauben; Konfiguration dokumentieren	Nachweis:	Dienstleister-Bestätigung + Kurzbeschreibung der Regeln
<i>Der Zugang der Praxis zum Internet muss so geschützt sein, dass niemand unbefugt von außen ins Praxisnetz kommt und nur erlaubte Verbindungen nach außen möglich sind.</i>			
A1-12 Dokumentation des Netzes			
Übersicht aller Geräte und Netzwerk erstellen			
Praxis:	Geräteliste liefern	Dokument:	Inventarliste A1-10
IT:	Netzplan ergänzen	Nachweis:	Netzplan abgelegt
<i>Es muss einen Plan geben, der zeigt, wie das Praxisnetz aufgebaut ist und welche Geräte verbunden sind.</i>			

A1-13 Grundlegende Authentisierung für den Netzmanagement-Zugriff			
Zugänge zur Netzwerkverwaltung absichern			
Praxis:	Verantwortliche benennen	Dokument:	IT-Termin
IT:	Sichere Zugänge einrichten	Nachweis:	Bestätigung Passwortablage
<i>Der Zugriff auf die Netzwerktechnik darf nur mit sicheren Anmeldedaten möglich sein.</i>			
A1-14 Installation von Updates			
Updates für PCs, Programme und Geräte zeitnah installieren			
Praxis:	Update-Turnus festlegen (z.B. monatlich) und Ansprechpartner benennen	Dokument:	Update-Regel + Zuständigkeit A1-09
IT:	Automatische Updates aktivieren wo möglich; regelmäßige Patch-Routine dokumentieren	Nachweis:	Dokumentierte Update-Regel + Bestätigung Dienstleister
<i>Aktualisierungen für Programme und Geräte müssen zeitnah eingespielt werden.</i>			
A1-15 Verantwortlichkeit für Updates			
Zuständigkeit für Updates festlegen			
Praxis:	Zuständigkeit schriftlich festlegen	Dokument:	Zuständigkeitsblatt A1-09
IT:		Nachweis:	Unterschriebenes Dokument
<i>Es muss klar festgelegt sein, wer für das Einspielen von Aktualisierungen zuständig ist und dafür geschult wurde.</i>			

A1-16 Identifizierung ausbleibender Updates			
Liste führen zu Support-Ende von Geräten/Programmen			
Praxis:	Liste pflegen	Dokument:	Inventarliste A1-10
IT:	Support-Ende prüfen	Nachweis:	Liste Ablaufdaten
	<i>Es muss erkannt werden, welche Geräte oder Programme keine Sicherheitsaktualisierungen mehr bekommen.</i>		
A1-17 Ausmusterung oder Separierung bei ausbleibenden Updates			
Alte Systeme ersetzen oder isolieren			
Praxis:	Entscheidung treffen	Dokument:	Maßnahmenplan
IT:	Technisch umsetzen	Nachweis:	Bestätigung Umsetzung
	<i>Geräte oder Programme ohne Sicherheitsupdates müssen ersetzt oder in einem getrennten Netz betrieben werden.</i>		
A1-18 Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras			
Kamera und Mikrofon nur bei Bedarf aktivieren			
Praxis:	Regel kommunizieren	Dokument:	Regelblatt
IT:	Technisch deaktivieren	Nachweis:	Dokumentierte Regel
	<i>Mikrofon und Kamera an Rechnern sollen normalerweise ausgeschaltet sein und nur kurzzeitig bei Bedarf eingeschaltet werden.</i>		

A1-19 Abmelden nach Aufgabenerfüllung			
Bildschirm sperren bei Verlassen			
Praxis:	Teamregel festlegen	Dokument:	Aushang
IT:	Automatische Sperre einstellen	Nachweis:	Screenshot Einstellung
<i>Nach der Arbeit am Gerät muss der Zugang gesperrt oder man muss sich abmelden.</i>			
A1-20 Einsatz von Virenschutzprogrammen			
Schutzprogramm gegen Schadsoftware auf allen Praxis-PCs einsetzen und überwachen			
Praxis:	Verantwortliche Person für Meldungen/Funde festlegen	Dokument:	Vertrag/Lizenz + Zuständigkeit
IT:	Schutzprogramm installieren, zentral verwalten, Updates aktivieren; Meldungen/Protokolle einrichten	Nachweis:	Lizenz/Vertrag + Dienstleister-Bestätigung + Zuständigkeitsnotiz
<i>Auf allen Geräten muss ein aktuelles Schutzprogramm gegen Schadsoftware installiert sein.</i>			
A1-21 Regelmäßige Datensicherung			
Regelmäßige Datensicherung durchführen			
Praxis:	Festlegen, welche Daten kritisch sind und wo sie liegen (Praxissoftware, Dokumente, Bilder)	Dokument:	Backup-Plan
IT:	Backup automatisieren; getrennt speichern; Protokoll/Benachrichtigung einrichten	Nachweis:	Backup-Konzept (Was/Wohin/Wie oft) + Bestätigung Dienstleister
<i>Wichtige Praxisdaten müssen regelmäßig gesichert werden.</i>			

A1-22 Schutz der Datensicherung			
Backups vor Zugriff schützen			
Praxis:	Aufbewahrungsort/Schlüsselverwaltung festlegen (z.B. Safe) und dokumentieren	Dokument:	Backup-Konzept
IT:	Backups verschlüsseln oder physisch/organisatorisch schützen; Zugriff beschränken	Nachweis:	Backup-Schutzkonzept + Bestätigung Dienstleister
<i>Die gesicherten Daten müssen so aufbewahrt werden, dass Unbefugte nicht darauf zugreifen können.</i>			
A1-23 Art der Datensicherung			
Sicherungsart und Turnus festlegen			
Praxis:	Plan erstellen	Dokument:	Backup-Plan
IT:		Nachweis:	Backup-Plan
<i>Es muss festgelegt sein, auf welche Weise die Datensicherung erfolgt.</i>			
A1-24 Verantwortliche der Datensicherung			
Zuständigkeit und Vertretung festlegen			
Praxis:	Dokumentieren	Dokument:	Zuständigkeitsblatt A1-11
IT:		Nachweis:	Unterschrift
<i>Es muss klar benannt sein, wer für die Datensicherung verantwortlich ist.</i>			

A1-25 Test der Datensicherung			
Wiederherstellung der Datensicherung regelmäßig testen (empfohlen)			
Praxis:	Test-Termine planen und Ergebnisse abheften	Dokument:	Testprotokoll A1-12
IT:	Test-Wiederherstellung durchführen/unterstützen	Nachweis:	Testprotokolle
	<i>Es muss regelmäßig geprüft werden, ob sich gesicherte Daten vollständig wiederherstellen lassen.</i>		
A1-26 Der Zugriff auf Geräte und Software muss abgesichert werden.			
Zugriffe in Praxissoftware nach Rollen vergeben			
Praxis:	Rollen definieren	Dokument:	Rollenmatrix, A1-13
IT:	Rechte setzen	Nachweis:	Screenshot/Bestätigung
	<i>Zugriffe auf Geräte und Patientendaten müssen über Benutzerkonten und Rollen geregelt sein, z.B. bei der Nutzung von Sicherheitskarten wie dem eHBA.</i>		
A1-27 Konfiguration von Synchronisationsmechanismen			
Keine private Cloud-Synchronisation auf Praxis-PCs			
Praxis:	Regel festlegen	Dokument:	IT-Termin
IT:	Einstellungen prüfen	Nachweis:	Bestätigung
	<i>Die automatische Synchronisierung von Daten mit Microsoft-Cloud-Diensten muss ausgeschaltet sein.</i>		

A1-28 Datei- und Freigabeberechtigungen			
Ordner- und Dateizugriffe passend vergeben			
Praxis:	Festlegen wer Zugriff braucht	Dokument:	Ordnerliste
IT:	Rechte setzen	Nachweis:	Berechtigungsliste
	<i>Zugriffe auf Dateien und Ordner müssen klar für Gruppen und einzelne Personen geregelt sein.</i>		

A1-29 Datensparsamkeit			
Nur notwendige Patientendaten speichern			
Praxis:	Löschroutine festlegen	Dokument:	Lösch-Regel
IT:		Nachweis:	Regel/Protokoll
	<i>Es sollen nur die wirklich notwendigen personenbezogenen Daten gespeichert und genutzt werden.</i>		

A1-30 Verwendung der SIM-Karten-PIN			
SIM-Karte mit PIN schützen			
Praxis:	PIN setzen	Dokument:	PIN-Notiz
IT:		Nachweis:	Ablageort dokumentiert
	<i>SIM-Karten müssen mit einer PIN geschützt sein. Die Entsperrnummer darf nur verantwortlichen Personen bekannt sein.</i>		

A1-31 Sichere Grundkonfiguration für mobile Geräte			
Mobilgeräte sicher konfigurieren			
Praxis:	Mobil-Check durchführen	Dokument:	Mobil-Checkliste
IT:		Nachweis:	Ausgefüllte Checkliste
<i>Mobile Geräte müssen von Anfang an mit den sichersten Einstellungen eingerichtet werden.</i>			
A1-32 Verwendung eines Zugriffsschutzes			
Gerätesperre mit Code/Biometrie			
Praxis:	Einstellen und prüfen	Dokument:	Kurzanleitung
IT:		Nachweis:	Stichprobe
<i>Mobile Geräte müssen mit einem sicheren Sperrcode geschützt sein.</i>			
A1-33 Datenschutz-Einstellungen			
App-Zugriffe einschränken			
Praxis:	Prüfen	Dokument:	Mobil-Check
IT:		Nachweis:	Checkliste
<i>Apps dürfen nur auf die Daten und Funktionen zugreifen, die unbedingt notwendig sind.</i>			

A1-34 Sperrmaßnahmen bei Verlust eines Mobiltelefons			
Notfallplan bei Handyverlust			
Praxis:	Notfallblatt erstellen	Dokument:	Notfallblatt
IT:		Nachweis:	Abgelegt
<i>Geht ein Mobiltelefon verloren, muss die SIM-Karte sofort gesperrt werden. Die Kontaktdaten des Anbieters müssen dafür bereitliegen.</i>			
A1-35 Nutzung der Sicherheitsmechanismen von Mobiltelefonen			
Sicherheitsfunktionen am Handy aktivieren			
Praxis:	Aktivieren	Dokument:	Mobil-Check
IT:	Optional MDM einrichten	Nachweis:	Screenshot/Bestätigung
<i>Alle vorhandenen Sicherheitsfunktionen des Mobiltelefons sollen aktiviert und genutzt werden.</i>			
A1-36 Schutz vor Schadsoftware			
USB-Datenträger vor Nutzung prüfen			
Praxis:	Regel festlegen	Dokument:	Regelblatt
IT:		Nachweis:	Regel
<i>Externe Datenträger müssen vor jeder Nutzung mit einem Schutzprogramm geprüft werden.</i>			

A1-37 Angemessene Kennzeichnung der Datenträger beim Versand			
Datenträger beim Versand neutral kennzeichnen			
Praxis:	Versandregel festlegen	Dokument:	Versandbuch
IT:		Nachweis:	Eintrag Versandbuch
<i>Beim Versand müssen Datenträger so gekennzeichnet sein, dass der Empfänger sie erkennt, Außenstehende aber nichts über den Inhalt erfahren.</i>			

A1-38 Sichere Versandart und Verpackung			
Sicherer Versand von Datenträgern			
Praxis:	Prozess festlegen	Dokument:	Versandbuch
IT:		Nachweis:	Versandnachweis
<i>Datenträger müssen mit einer sicheren und möglichst manipulationsgeschützten Versandart verschickt werden.</i>			

A1-39 Sicheres Löschen der Datenträger vor und nach der Verwendung			
Falls Datenträger genutzt werden: Datenträger nach Verwendung sicher löschen			
Praxis:	Regel: nur freigegebene Datenträger; Rückgabe/Entsorgung dokumentieren	Dokument:	Löschanweisung + Löschprotokoll
IT:	Sichere Löschung durchführen oder Verfahren/Tool bereitstellen	Nachweis:	Löschprotokolle (bei Bedarf)
<i>Datenträger müssen nach der Nutzung vollständig und sicher gelöscht werden.</i>			

A1-40 Sichere Konfiguration der E-MailClients			
E-Mail-Programm sicher konfigurieren			
Praxis:		Dokument:	IT-Termin
IT:	Sichere Einstellungen vornehmen	Nachweis:	Bestätigung
<i>E-Mail-Anhänge müssen vor dem Öffnen geprüft werden. Aktive Inhalte in E-Mails sollen deaktiviert sein. Die Verbindung zum E-Mail-Server muss verschlüsselt erfolgen.</i>			
A1-41 Umgang mit Spam durch Benutzer			
Umgang mit Spam/Phishing schulen			
Praxis:	Schulung durchführen	Dokument:	1-Seiter Anleitung
IT:		Nachweis:	Teilnahmeliste
<i>Unerwünschte E-Mails sollen gelöscht werden. Es darf nicht geantwortet und keine Links darin geöffnet werden.</i>			
A1-42 Sichere Apps nutzen			
Apps nur aus offiziellen App-Stores installieren; ungenutzte Apps samt Konto/Daten entfernen			
Praxis:	Teamregel umsetzen; regelmäßige App-Überprüfung (löschen, wenn nicht benötigt)	Dokument:	Regelblatt
IT:		Nachweis:	Regel + kurze App-Liste (falls dienstliche Geräte)
<i>Apps dürfen nur aus offiziellen App-Stores installiert werden. Nicht mehr benötigte Apps müssen mit allen Daten und Benutzerkonten entfernt werden.</i>			

A1-43 Sichere Speicherung lokaler AppDaten			
Nur Apps mit sicherer Datenspeicherung nutzen			
Praxis:	Auswahlregeln festlegen	Dokument:	App-Liste
IT:		Nachweis:	Dokumentierte Freigabe
	<i>Es dürfen nur Apps genutzt werden, die gespeicherte Daten auf dem Gerät verschlüsselt ablegen.</i>		
A1-44 Verhinderung von Datenabfluss			
App-Berechtigungen auf Minimum beschränken			
Praxis:	Prüfen	Dokument:	Mobil-Check
IT:		Nachweis:	Checkliste
	<i>Die Zugriffe von Apps auf vertrauliche Daten müssen in den Einstellungen so weit wie möglich eingeschränkt werden.</i>		
A1-45 Authentisierung bei Webanwendungen			
Falls Webdienst: Zugriff nur mit Anmeldung			
Praxis:		Dokument:	IT-Projekt
IT:	Technisch umsetzen	Nachweis:	Dokumentation
	<i>Wenn die Praxis einen Webdienst anbietet, muss sich jeder Nutzer anmelden, bevor er auf geschützte Bereiche zugreift. Es muss eine sichere Anmeldemethode genutzt und die Anzahl falscher Anmeldeversuche begrenzt werden.</i>		

A1-46 Schutz vertraulicher Daten			
Falls Webdienst: Passwörter sicher speichern und Webdienst-Dateien vor Zugriff schützen			
Praxis:		Dokument:	IT-Projekt + Dienstleister-Nachweis
IT:	Webdienst so betreiben, dass Passwörter sicher gespeichert sind und Systemdateien geschützt sind; schriftlich bestätigen	Nachweis:	Bestätigung
	<i>Zugangsdaten zu Webdiensten müssen sicher gespeichert sein, sodass Unbefugte sie nicht lesen können. Die Programmdateien des Dienstes müssen vor unbefugtem Zugriff geschützt sein.</i>		
A1-47 Einsatz von Web Application Firewalls			
Falls Webdienst: Zusätzlicher Schutz vor Angriffen auf den Webdienst (empfohlen)			
Praxis:		Dokument:	IT-Projekt
IT:	Geeigneten Zusatzschutz einrichten und nach Updates prüfen; schriftlich bestätigen	Nachweis:	Bestätigung
	<i>Zum Schutz von Webdiensten soll eine spezielle Schutzlösung eingesetzt und nach Änderungen am Webdienst angepasst werden.</i>		
A1-48 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen			
Falls Webdienst: Schutz vor automatisierter Nutzung			
Praxis:		Dokument:	IT-Projekt
IT:	Technisch umsetzen	Nachweis:	Bestätigung
	<i>Webdienste müssen davor geschützt werden, dass Programme sie unberechtigt automatisch nutzen, ohne berechnigte Nutzer zu behindern.</i>		

A1-49 Kryptografische Sicherung vertraulicher Daten			
Falls Webdienst: Verschlüsselte Verbindung (https)			
Praxis:		Dokument:	IT-Projekt
IT:	Technisch umsetzen	Nachweis:	Zertifikatsnachweis
	<i>Bei der Nutzung von Webanwendungen muss darauf geachtet werden, dass die Verbindung verschlüsselt ist (https).</i>		

A1-50 Sicherheit von Cloud-Dienstleistern			
Falls Patientendaten in der Cloud verarbeitet werden: Anbieter-Nachweis nach Gesetz (C5) prüfen und ablegen			
Praxis:	Prüfen, ob Patientendaten in einer Cloud liegen; Nachweis ablegen	Dokument:	Anbieterunterlagen
IT:	C5-Nachweis einholen, Aktualität prüfen, schriftlich bestätigen	Nachweis:	C5-Nachweis
	<i>Wenn Gesundheitsdaten in einer Cloud verarbeitet werden, darf nur ein Anbieter genutzt werden, der ein aktuelles C5-Sicherheitszertifikat besitzt.</i>		