Dr. BERKANT OMAN

PERSONALINFORMATIONSTECHNOLOGIEN

NUTZUNGSRICHTLINIEN

Adresse : Kazımdirik Mah. 372/9 Sokak Nr. 1 Bornova/İzmir

Telefon : +90 552 361 49 88

Netz : https://www.drberkantoman.com/

Email : oman.klinik@gmail.com

INHALT

DR. BERKANT OMAN-PRÜFUNG PERSÖNLICHE INFORMATIONSTECHNOLOGIEN-NUTZUNGSRICHTLINIEN

Veröffentlichungsdatum	: 10.05.2021
Sicherheit	: ALLGEMEINER GEBRAUCH
Zugehöriges Dokument	: IT-Sicherheitsrichtlinie
Eigentümer und Update-Manager.	: Abteilung für Informationstechnologien
Pflichten und Verantwortlichkeiten	: Management, Managementvertreter, Alle Mitarbeiter

Abkürzungen:

IT: IT / IT P2P: Ende-zu-Ende-Verbindung VPN: virtuelles privates Netzwerk

W-lan: Kabellos

1. ZIEL:

In den Informationssystemen unserer Praxis befinden sich sehr wichtige Informationen und es ist von großer Bedeutung, die Sicherheit, Vertraulichkeit und Privatsphäre dieser Informationen zu schützen. Eine Sicherheitslücke in einem mit dem Netzwerk verbundenen Computer kann dazu führen, dass die Sicherheit aller Informationssysteme unserer Praxis gefährdet ist.

2. UMFANG:

Sicherheitsmaßnahmen auf allgemeiner System- und Nutzungsebene, um Störungen der Sicherheit der Informationssysteme unserer Praxis zu verhindern

Darüber hinaus gibt es einige Regeln, die unsere Mitarbeiter diesbezüglich sorgfältig befolgen müssen. Das gesamte Praxispersonal hat sich an diese Regeln zu halten.

Der Benutzer ist für alle Schäden und negativen Folgen verantwortlich, die bei Nichtbeachtung dieser Regeln entstehen können. Nachfolgend sind die einzuhaltenden Regeln aufgeführt.

3. E-MAIL-NUTZUNGSREGELN

A. Das E-Mail-System der Praxis darf niemals für böswillige oder persönliche Zwecke genutzt werden, um Nachrichten zu versenden, die Inhalte enthalten, die darauf abzielen, die Rechte des Empfängers zu belästigen, zu missbrauchen oder in irgendeiner Weise zu verletzen.

B. Kettennachrichten und E-Mails, die an Nachrichten angehängte ausführbare Dateien enthalten, sollten sofort nach Erhalt gelöscht und niemals an andere weitergeleitet werden.

C. Klinik-E-Mail-Adressen sollten nicht zum Abonnieren von Listen im Internet für den persönlichen Gebrauch verwendet werden.

C. Spam, Ketten-E-Mails, gefälschte E-Mails usw. Auf schädliche E-Mails sollte nicht geantwortet werden. Gleichzeitig darf die E-Mail-Adresse der Praxis nicht zum Versenden von Spam- und Phishing-Nachrichten an andere Nutzer innerhalb und außerhalb der Praxis genutzt werden.

D. Da es sich bei E-Mails, in denen Benutzer zur Eingabe ihres Benutzercodes/Passworts aufgefordert werden, um gefälschte E-Mails handeln kann, sollten sie sofort und ohne Maßnahmen gelöscht werden.

Zu. Mitarbeiter, per E-Mail unangemessene Inhalte (Pornografie, Rassismus, politische Propaganda, geistiges Eigentum usw.) und alle Benutzer und Gruppen innerhalb und außerhalb der Praxis; Sie dürfen keine E-Mails versenden, die verleumderisch, beleidigend oder schädlich sind.

F. Mitarbeiter müssen verhindern, dass ihre Nachrichten von Unbefugten gelesen werden. Daher sollten Passwörter verwendet und Hardware-/Softwaresysteme für den E-Mail-Zugriff vor unbefugtem Zugriff geschützt werden.

G. Da es sich bei E-Mails, in denen Benutzer zur Eingabe ihres Benutzercodes/Passworts aufgefordert werden, um gefälschte E-Mails handeln kann, sollten sie sofort und ohne Maßnahmen gelöscht werden.

G. Das Praxispersonal sollte seine Nachrichten regelmäßig überprüfen und sollte auf Ihre Nachrichten antworten.

H. Das Klinikpersonal ist dafür verantwortlich, dass Firmen-E-Mails nicht von Außenstehenden und Unbefugten eingesehen und gelesen werden können.

I. Dateien in E-Mail-Anhängen unbekannter Herkunft sollten niemals geöffnet und sofort gelöscht werden. Denn diese E-Mails können schädlichen Code wie Viren, E-Mail-Bomben und Trojanische Pferde enthalten.

I. Praxismitarbeiter sollten in der Post, die sie senden, empfangen oder speichern, nicht nach Persönlichkeiten suchen. Im Falle rechtswidriger und beleidigender E-Mail-Kommunikation können autorisierte Personen die E-Mail-Nachrichten kontrollieren und ohne vorherige Ankündigung rechtliche Schritte gegen den Nutzer einleiten.

J. Es dürfen keine „sensiblen“ oder „vertraulichen“ Dokumente der Praxis im Klartext an irgendjemanden gesendet werden, auch nicht an die privaten E-Mail-Adressen der Nutzer.

k. Der Nutzer ist für die Sicherheit des Passworts seiner E-Mail-Adresse und die rechtlichen Konsequenzen, die sich aus den versendeten E-Mails ergeben, verantwortlich. Sobald sie feststellen, dass ihre Passwörter geknackt wurden, sind sie verpflichtet, sich an die Behörden zu wenden und den Vorfall zu melden.

4. PASSWORTRICHTLINIE

A. Alle Passwörter auf Benutzerebene (z. B. E-Mail, Web, Laptop, Desktop-Computer usw.) sollten mindestens alle 6 Monate geändert werden. Der empfohlene Austauschzeitraum beträgt alle vier Monate.

B. Passwörter sollten nicht an E-Mail-Nachrichten oder andere elektronische Formulare angehängt werden.

C. Passwörter sollten nicht an Dritte weitergegeben und nicht auf Papier oder elektronischen Medien geschrieben werden.

C.Bei der Verschlüsselung können Sie Klein- und Großbuchstaben (Beispiel: az, AZ), sowohl Zahlen als auch Satzzeichen sowie Buchstaben (Beispiel: 0-9 !@ ^+%&*()_+|=%&/) verwenden. ()?,. /) muss gefunden werden.

D. Es muss mindestens acht alphanumerische Zeichen (Buchstaben, Zahlen und Satzzeichen) enthalten.

Zu. In keiner Sprache sollte es umgangssprachliche Wörter geben.

F. Familiennamen sollten nicht verwendet werden.

G. Niemand sollte am Telefon ein Passwort erhalten.

G. Passwörter sollten nicht an Dritte weitergegeben werden, auch nicht an Familienmitglieder.

H. Geben Sie Ihre Passwörter nicht an Ihre Kollegen weiter, wenn Sie nicht am Arbeitsplatz sind.

I. Ein Benutzername und ein Passwort sollten nicht auf mehr als einem Computer gleichzeitig verwendet werden.

I. Das Knacken und Erraten von Passwörtern kann von der IT-Abteilung regelmäßig durchgeführt werden. Sollten durch den Sicherheitsscan Passwörter erraten oder geknackt werden, wird der Benutzer aufgefordert, sein Passwort zu ändern.

J. Alle Arten von Dokumenten, die per Büro-E-Mail versendet werden sollen, müssen komprimiert und verschlüsselt sein. Die Passwortübermittlung erfolgt telefonisch, nicht per E-Mail.

k. Ist bei der USB-Nutzung in der Praxis die Speicherung eines Dokuments auf USB erforderlich, muss dieses komprimiert und verschlüsselt gespeichert werden. Das oben Genannte gilt für USB-Geräte oder andere tragbare Geräte und sollte nur bei Bedarf und mit IT-Kenntnissen durchgeführt werden.

5. ANTIVIRUS-POLITIK

A. Antivirensoftware sollte auf dem gesamten Computer installiert sein und automatisch aktualisiert werden.

B. Computer ohne installierte Antivirensoftware sollten nicht mit dem Netzwerk verbunden werden.

C. Das Erstellen und Verbreiten schädlicher Programme (z. B. Viren, Würmer, Trojaner, E-Mail-Spam usw.) innerhalb der Praxis ist untersagt.

C. Kein Benutzer sollte das Antivirenprogramm aus irgendeinem Grund vom System entfernen. lässt sich nicht heben.

D. Das Antivirenprogramm muss auf jedem neu installierten Betriebssystem installiert werden.

6. INTERNETNUTZUNGSRICHTLINIE

A. Kein Benutzer kann die Dienste zum Herunterladen und Hochladen von Dateien im Internet über eine P2P-Verbindung nutzen. (Probe:*Unfall, Torrent, Imesh, Edonkey*usw.)

B. Im Computernetzwerk, außer bei Bürogesprächen*ICQ, MIRC, Messenger*usw. wie Messaging- und Chat-Programme*Plaudern*Programme werden nicht verwendet und*Plaudern*Dateien sollten nicht über Programme ausgetauscht werden.

C. Kein Nutzer darf das Internet zu anderen Zwecken als zur geschäftlichen Kommunikation nutzen. *Multimedia-Streaming*(Video-Sharing und Audio-/Video-Übertragung)

werde nicht in der Lage sein zu.

C. Es ist verboten, während der Arbeitszeit übermäßig nicht arbeitsbezogene Websites zu durchsuchen. (Probe:*Facebook, Youtube*)

D. Senden von Dateien mit hohem Volumen (Musik-, Videodateien), die nicht mit der Arbeit zusammenhängen (*hochladen*) und herunterladen (*herunterladen*) ist verboten.

Zu. Software, die nicht von der IT-Abteilung genehmigt wurde, kann nicht über das Internet heruntergeladen werden diese Software nicht auf den Praxissystemen installiert und genutzt werden kann,

F. Es ist verboten, Websites zu betreten, die gegen die allgemeine Moral verstoßen, und Dateien über Computer herunterzuladen.

G. Das Herunterladen und Kopieren aller Arten von Programmen wie Bildschirmschonern, Desktop-Bildern und Tools, die als Dienstprogramme bezeichnet werden, über das Internet ist verboten, da sie die Betriebssysteme von Computern in hohem Maße gefährden.

G. Die Nutzung des Internets durch Dritte aus der Praxis heraus kann mit Zustimmung des IT-Verantwortlichen und den diesbezüglichen Regelungen erfolgen.

H. Um Arbeitsplatzverlusten vorzubeugen, werden von der Praxis Beobachtungen und statistische Untersuchungen über die Internetnutzung der Mitarbeiter durchgeführt.

7. CLEAN TABLE CLEAN SCREEN-RICHTLINIE

A. Am Ende der Arbeitszeit bleiben keine Dokumente auf dem Schreibtisch liegen, sondern werden in verschlossenen Schubladen oder Schränken abgelegt, die üblicherweise zu Bürotischen gehören.

B. Vor längerem Verlassen des Büros werden die Unterlagen auf dem Schreibtisch und den Peripheriegeräten gereinigt. Wichtige Dokumente werden in Schränken und verschlossenen Schubladen aufbewahrt. Das Personal ist verpflichtet, physische Dokumente vor möglichen Gefahren (Verschütten von Flüssigkeiten, Verbrennen, Zerstörung) zu schützen.

C. Kleine Zettel mit Passwort und Benutzername werden nicht auf oder in der Nähe des Arbeitstisches zurückgelassen.

C. Um die Anzahl der Desktop-Dokumente nicht zu erhöhen, wird darauf geachtet, elektronische Dokumente möglichst nicht über den Drucker auszudrucken.

D. Anstatt gedruckte Dokumente „nach Bedarf“ auf dem Desktop zu speichern, ist es sinnvoller, elektronische Kopien dieser Dokumente von Scannern zu erstellen und diese auf dem Computer zu sichern und das Dokument selbst entweder zu vernichten oder zu archivieren.

Zu. Es sollte darauf geachtet werden, die Papiere im Aktenvernichter zu zerkleinern, anstatt sie in den Aktenvernichter zu werfen Mülleimer.

F. Auch bei kurzfristigen Abreisen sollten Gegenstände wie Mobiltelefone, PDAs, USB-Sticks, externe Festplatten, CDs, DVDs nicht auf dem Arbeitstisch liegen bleiben.

G. Bei kurzfristigen Abreisen bleiben Dokumente ohne wertvolle Informationen nicht auf dem Schreibtisch liegen, sondern werden in verschlossenen Schubladen aufbewahrt.

G. Visitenkartenboxen, persönliche Tagebücher, Kontoauszüge, Schecks auf dem Tisch Dokumente mit wertvollen Informationen wie Notizbücher bleiben nicht liegen, sondern werden in verschlossenen Schubladen aufbewahrt.

H. Neben Dokumenten sollten beim kurz- oder längerfristigen Verlassen des Schreibtisches auch Computerbildschirme ausgeschaltet oder ein passwortgeschützter Bildschirmschoner aktiviert werden.

I. Die Schlüssel von Schreibtischschubladen, private Schlüssel wie Haus- und Autoschlüssel sowie Safeschlüssel sollten nicht auf dem Tisch liegen bleiben.

8. SOZIALTECHNIK-SCHUTZPOLITIK

A. Dabei handelt es sich um eine Möglichkeit, Informationen durch verschiedene Überredungs- und Täuschungsmethoden zu erhalten, die auf Menschen abzielen Schwächen statt der Einsatz von Technologie.

B. Erfindet falsche Szenarien und überzeugt ihn davon, dass er eine zuverlässige Quelle ist (*Phishing*), Trojanische Pferde, Geld, Geschenke usw. im Austausch gegen verlässliche Informationen. Dabei kommen Angriffsmethoden wie Andeutungen, Vertrauensgewinnung und Informationsbeschaffung zum Einsatz.

C. Sie können Social-Engineering-Angriffen innerhalb der Organisation, außerhalb der Organisation oder sogar zu Hause ausgesetzt sein. Gleiches gilt für verschiedene Kommunikationsmedien wie Telefon, Fax, E-Mail, Telefonkonferenz. Gefahr kann von einem Ort ausgehen, den Sie am wenigsten erwarten, und zwar dann, wenn Sie sie am wenigsten erwarten. Wenn Sie mit ungewöhnlichen Situationen konfrontiert werden, denken Sie zweimal darüber nach, bevor Sie Maßnahmen ergreifen. Möglicherweise geraten Sie in eine große Falle.

C. Seien Sie vorsichtig bei Anfragen von Personen, die Sie nicht kennen. Mit Telefon

Wenn Sie angerufen werden, fragen Sie nach der Telefonnummer des Gesprächspartners. Wenn es sich um ein persönliches Treffen handelt, fragen Sie nach der Adresse oder Telefoninformationen.

D. Beenden Sie den Anruf sofort, wenn eine der folgenden Situationen eintritt:

- Betonen Sie, dass es schlimme Folgen haben wird, wenn der Bitte nicht nachgekommen wird.
- Außergewöhnliche Ansprüche stellen
- Genervt sein, wenn man Fragen stellt
- Anspruch auf Autorität erheben
- Listen Sie nacheinander die Namen auf, die sich auf das Thema beziehen, das Sie kennen
- Betonung der Dringlichkeit der Situation
- Komplimente machen oder umwerben
- Geben Sie Ihre privaten Daten (z. B. Ihr Passwort) nicht an Dritte weiter.
- Systemadministrator
- Ihr Kollege sitzt am Nebentisch
- Sogar Ihre Manager

- Geben Sie keine Informationen über Ihre Computerkonten und Passwörter weiter, auch wenn die Anfragen von einer E-Mail-Adresse und Telefonnummer stammen, die Sie kennen, kennen und denen Sie vertrauen.
- Öffnen Sie keine betrügerischen E-Mails an Ihre E-Mail-Adresse. Klicken Sie nicht auf die in dieser E-Mail gesendeten Links, laden Sie keine Bilder herunter und antworten Sie nicht auf E-Mails, auch wenn Sie diese geöffnet haben.
- Kein Institutions- oder Website-Administrator benötigt Ihre Anmeldeinformationen, da es bereits ein „Site-Administrator"-Panel (Administrator) gibt, das bereit ist, Änderungen oder Aktionen an Ihrer Mitgliedschaft oder Ihrem Konto vorzunehmen. Aus diesem Grund geben Sie Ihre Mitgliedsdaten und natürlich Ihr Passwort usw. nicht an Personen weiter, die sich als Administrator oder Websitebesitzer ausgeben. du solltest nicht.
- Wenn jemand Ihren schwachen Moment ausnutzen möchte, indem er Sie ängstlich oder aufgeregt macht, indem er Sie glauben lässt, Sie hätten ein Verbrechen begangen oder einen Preis gewonnen, sollten Sie das wissen; Kein Beamter bittet Sie am Telefon oder per E-Mail um Geld, um Sie aus der Situation zu retten, in der Sie sich befinden, und ebenso bittet niemand die Person, Geld auf ein bestimmtes Konto oder Telefon zu überweisen.
- Verwenden Sie keine Raubkopien von Programmen, Musik oder Videos auf Ihrem Computer, besuchen Sie keine Glücksspielseiten und ähnliche schädliche Websites.

9. MOBILE COMPUTING-POLITIK

A. Tragen Sie Ihr Telefon immer bei sich. Lassen Sie ihn nicht unbeaufsichtigt. Vermeiden Sie es, Ihr Telefon überall zur Schau zu stellen. Wenn Sie mit dem Auto anreisen, stellen Sie sicher, dass Sie beim Verlassen des Fahrzeugs mobile Geräte dabei haben.

B. Verwenden Sie immer den Sicherheitssperrcode oder die PIN-Codes Ihres Telefons und halten Sie diese geheim. Machen Sie diese Codes zu etwas Besonderem für Sie, indem Sie das Passwort und die PIN-Codes in den vordefinierten Werkseinstellungen immer ändern.

C. Es ist strengstens verboten, die Werkseinstellungen des Telefons und die Einstellungen des Betriebssystems durch Vorgänge wie Jailbreaking, Rooting oder Hacking zu ändern. Dies macht das Smartphone zwar anfälliger für Cyberangriffe, schwächt jedoch die Sicherheitsfunktionen, die der Betreiber und das Smartphone bieten.

C. Autorisierung von Anwendungen zum Zugriff auf Ihre persönlichen Daten auf Ihren Smartphones
Es wird empfohlen, vorsichtig zu sein. Andernfalls haben Sie möglicherweise mit der von Ihnen heruntergeladenen Anwendung der Verarbeitung Ihrer personenbezogenen Daten (z. B. Ihrer Standortdaten) zugestimmt. Überprüfen Sie außerdem unbedingt die Datenschutzeinstellungen für jede App, bevor Sie sie installieren.

D. Vor dem Herunterladen einer App sollte eine Recherche durchgeführt werden, um sicherzustellen, dass die App legitim und zuverlässig ist. Es wird dringend empfohlen, Anwendungen zum Herunterladen auf Smartphones aus der offiziellen Anwendungsumgebung des Betriebssystems zu beziehen.

Zu. Sie können damit sogar aus der Ferne auf alle auf Ihrem Telefon gespeicherten Daten zugreifen und diese löschen wenn das GPS des Telefons ausgeschaltet ist, mit der Anwendung, die als Anwendung auf Smartphones bezogen oder über das Practice MDM installiert werden kann. Wenn Sie in diesem Fall Ihr Telefon verlieren, aktivieren einige Apps möglicherweise einen lauten Alarm, auch wenn Ihr Telefon stumm geschaltet ist. Diese Apps können Ihnen auch dabei helfen, Ihr Telefon leichter zu finden, wenn Sie es verlieren.

F. Deaktivieren Sie Bluetooth, WLAN und andere Dienste, wenn Sie sie nicht verwenden.

G. Durch die Aktivierung automatischer Updates müssen Sie das Betriebssystem Ihres Telefons auf dem neuesten Stand halten oder Updates von Ihrem Dienstanbieter, Betriebssystemanbieter, Gerätehersteller und Anwendungsanbieter akzeptieren. Indem Sie Ihr Betriebssystem auf dem neuesten Stand halten, können Sie das Risiko einer Gefährdung durch Cyber-Bedrohungen verringern.

G. Wenn Ihr Telefon über eine Datenverschlüsselungsfunktion verfügt, stellen Sie sicher, dass Sie diese Funktion verwenden. Wenn wir über eine solche Funktion nicht verfügen, wird empfohlen, eine Datenverschlüsselungsanwendung zu verwenden. Im Falle eines Diebstahls oder Verlusts des Telefons werden die Daten, selbst wenn sie erfasst werden, von der betroffenen Person nicht verwendet und nicht verstanden.

H. Wenn Ihr Telefon gestohlen wird oder verloren geht, wenden Sie sich an die Abteilung für Informationstechnologien der Praxis, um Ihren Telefonanschluss abzuschalten. Um die Nutzung Ihres Telefons in unserem Land zu verhindern, können Sie die Situation der Information Technologies and Communication Authority (BTK) (www.btk.gov.tr) melden.

I. Markieren (zeichnen) Sie die SIM-Karte, die zusätzliche Speicherkarte, den Akku und das Telefon mit einem physischen und für Fremde unsichtbaren Zeichen (zeichnen Sie ein kleines Zeichen, Buchstaben oder Zahlen oder versuchen Sie es mit ultravioletter Farbe, die bei normalem Licht unsichtbar ist).

I. Stellen Sie sicher, dass Sie wissen, welche Informationen auf Ihrer SIM-Karte, der zusätzlichen Speicherkarte und dem Telefonspeicher gespeichert sind. Speichern Sie keine vertraulichen Informationen auf Ihrem Telefon.

J. Schützen Sie Ihre SIM- und zusätzliche Speicherkarte. Stellen Sie sicher, dass Sie Ihre SIM-Karte und zusätzliche Speicherkarte nicht dort liegen lassen, wenn Sie Ihr Telefon warten.

k. Notieren Sie Ihre 15-stellige Seriennummer oder IMEI-Nummer. Dies hilft dabei, Ihr Telefon zu orten und sein Eigentum zu schützen, falls es verloren geht oder gestohlen wird.

l. Beachten Sie die Internetnutzungsrichtlinie, wenn Sie Ihr Telefon und andere tragbare Geräte verwenden.

10. RICHTLINIE ZUM FERNENARBEIT

A. Wenn Sie an öffentlichen Orten oder in der Praxis, in der Sie sich aufhalten, einen öffentlichen Internetzugang (Wi-Fi) nutzen, ist die Verwendung eines VPN erforderlich.

B. Der unverschlüsselte öffentliche drahtlose Netzwerkverkehr kann von der Person, die diesen Dienst kostenlos anbietet, abgehört werden. Sie sollten die Nutzung öffentlicher Netzwerke einschränken und stattdessen eine sichere WLAN- oder drahtlose Mobilfunkverbindung von einem Anbieter verwenden, dem Sie vertrauen können.

C. Lassen Sie die Dateifreigabefunktionen Ihres PCs ausgeschaltet und Ihre Firewall (*Firewall*) ist immer eingeschaltet (ON).

C. Bewahren Sie keine Dateien mit vertraulichen Informationen auf Ihrem Computer auf. Wenn Sie es behalten müssen, behalten Sie es in Google Drive (Cloud). Wenn Sie sie auf dem lokalen Computer aufbewahren müssen, was wir nicht empfehlen, speichern Sie Ihre vertraulichen Informationen in einem Bereich, der durch Festplattenverschlüsselungssoftware geschützt ist.

D. Um das Risiko eines Diebstahls oder Verlusts Ihres Geräts zu vermeiden, sollten Ihre mit der Übungsanwendung und den Serverkonten verknüpften Passwörter nicht auf dem Computer gespeichert werden. Wenn Sie einer solchen Situation ausgesetzt sind, benachrichtigen Sie unverzüglich die zuständigen Behörden.

Zu. Die Computer der Benutzer arbeiten, indem sie eine Verbindung zum Remote Practice-Netzwerk herstellen zu bestimmten Zeiten kontrolliert werden. Diese Prüfungen umfassen Folgendes.

✓ Melden Sie sich an und verwenden Sie mit eingeschränktem Benutzer anstelle eines lokalen Administrators auf Computern.

✓ Updates von Windows und Antivirus-Anwendungen.

✓ Nicht lizenzierte oder bösartige Apps.

✓ Virusscan

11. ALLGEMEINE NUTZUNGSRICHTLINIEN

A. Alle PCs und Laptops sollten spätestens innerhalb von 15 Minuten automatisch auf den Passwort-Bildschirmschutz umschalten können.

B. Laptops sollten sorgfältiger vor Sicherheitslücken geschützt werden. Betriebssystem-Passwörter müssen aktiviert sein.

C. Falls der Laptop gestohlen wird oder verloren geht, sollten der IT-Beauftragte und die Personalabteilung so schnell wie möglich benachrichtigt werden, sobald die Situation bemerkt wird.

C. Alle Mobiltelefone, Smartphones, Tablets, tragbaren Geräte usw. Passwörter müssen aktiv sein, unabhängig davon, ob sie mit dem Netzwerk des Büros synchronisiert sind oder nicht.
Die Funktionen für den drahtlosen Zugriff (Infrarot, Bluetooth usw.) sind aktiv, wenn sie nicht verwendet werden.

sollten nicht mit Antiviren-Anwendungen vor Viren der neuen Generation geschützt werden und sollten nach Möglichkeit geschützt werden.

D. Alle Benutzer sind für die Sicherheit ihres Computersystems verantwortlich. Für Angriffe auf die Situation und Person (z. B. Electronic Banking etc.), die von diesen Computern ausgehen können, ist der Besitzer des Geräts verantwortlich.

Zu. Bei Bedarf (Krankheit, Meldung, Entlassung usw.) können Computer, Telefone, mobile Geräte usw. Den Abteilungsleitern sollten bei Bedarf Sicherheitspasswörter mitgeteilt werden. Wenn das entsprechende Personal an seinen Arbeitsplatz zurückkehrt, muss es das von ihm unterschlagene Gerätepasswort ändern.

F. Belästigungen oder illegale Aktivitäten dürfen bei der Nutzung der Praxiscomputer nicht erfolgen.

G. Störung der Netzwerksicherheit (zum Beispiel: Eine Person möchte unautorisiert auf Server zugreifen) oder der Netzwerkkommunikation (*Paket-Sniffing, Paket-Spoofing, Denial-of-Service*usw.) sollten keine Maßnahmen ergriffen werden.

G. Port- oder Netzwerkscans sollten nicht von Benutzern durchgeführt werden.

H. Beteiligen Sie sich nicht an Aktivitäten, die die Netzwerksicherheit gefährden.*BRUSTSTÜCK*Angriff, Port, Netzwerkscan usw. sollten nicht durchgeführt werden.

I. Wenn ihm ein Informationssicherheitsvorfall auffällt, sollte er den IT-Mitarbeiter unverzüglich benachrichtigen.

I. Praxisinformationen sollten nicht an Dritte außerhalb der Praxis weitergegeben werden.

J. Ohne Genehmigung des IT-Verantwortlichen darf kein Peripherieanschluss an den Personalcomputern der Benutzer vorgenommen werden.

k. Sollten in der Praxis genutzte Geräte wie z. B. USB verloren gehen oder gestohlen werden, ist dies umgehend dem IT-Beauftragten zu melden.

l. Geräte, Software und Daten dürfen nicht ohne Genehmigung aus der Einrichtung mitgenommen werden.

M. Es ist verboten, Programme unbekannter Herkunft (Zeitschriften-CDs oder aus dem Internet heruntergeladene Programme etc.) zu installieren und zu nutzen, mit Ausnahme der in der Praxis verwendeten Software.

N. Unbefugtem Personal ist es untersagt, vertrauliche und sensible Informationen in der Praxis einzusehen oder zu erhalten.

Er. Besonderes Augenmerk sollte auf die Vertraulichkeit oder Privatsphäre von Unternehmens- oder Unternehmensdaten gelegt werden persönliche Daten. Diese Daten können unbeschadet der gesetzlichen Bestimmungen der Praxis nicht an Dritte und Institutionen in elektronischer oder Papierumgebung weitergegeben werden.

Er. Die Klinikmitarbeiter sind für den Schutz der institutionellen Informationen entsprechend verantwortlich unterliegen dem Grundsatz der Verschwiegenheit, solange es sich um Praxispersonal handelt und für den Fall, dass sie die Praxis verlassen (Pensionierung, Rücktritt etc.).

P. Dem Personal ist es untersagt, die Unternehmensinformationen auf den ihm zugewiesenen Desktop- und Laptop-Computern, die für die Unternehmensarbeit verwendet werden, regelmäßig auf verschiedenen Medien (CD, DVD, USB, externe Festplatte usw.) zu sichern.

R. Von der IT benannte autorisierte Personen können vor Ort oder aus der Ferne auf den Computer des Mitarbeiters zugreifen und Sicherheits-, Wartungs- und Reparaturarbeiten durchführen, ohne den Benutzer darüber zu informieren. In diesem Fall ist es autorisiertem Personal, das Fernwartungs- und Supportdienste anbietet, nicht gestattet, persönliche oder Unternehmensinformationen auf Personalcomputern einzusehen, zu kopieren oder zu ändern.

S. Spiele und Unterhaltungsprogramme sollten nicht auf Computern ausgeführt oder kopiert werden.

S. Mit Ausnahme von Praxisunterlagen und genehmigten Anträgen sollten keine Dateien am Computer ausgetauscht werden.

T. Ohne das Wissen der verantwortlichen IT-Person in den Gebäuden verfügen Computer nicht über Netzwerkeinstellungen, Benutzerdefinitionen, Ressourcenprofile usw. Die bestehenden Regelungen dazu sollten nicht geändert werden.

u. Nicht lizenzierte Programme sollten auf keinen Fall auf Computern installiert werden.

u. Computerressourcen sollten nicht gemeinsam genutzt werden, es sei denn, dies ist erforderlich. Ihre Ressourcen Beim Teilen müssen die Regeln für die Verwendung von Passwörtern eingehalten werden.

v. Vergessen wir nicht, dass das gesamte Praxispersonal, insbesondere der Eigentümer der Informationen, für die Informationssicherheit verantwortlich ist. Aus diesem Grund ist die Teilnahme an der Information Security Awareness Schulung, die einmal im Jahr stattfindet, für alle Mitarbeiter verpflichtend.