So handeln Sie richtig

am Arbeitsplatz

Melden Sie JEDEN verdächtigen Vorfall und ignorieren Sie nie mögliche Gefahren, die damit verbunden sind!

Home-Office

ARS DOCENDI ACADEMY

ARS DOCENDI ACADEMY

Sichere Arbeitsumgebung schaffen!

Sorgen Sie für ein sicheres Arbeitsumfeld. Schließen Sie Ihren Computer immer an ein geschütztes Netzwerk an und verwenden Sie eine sichere Verbindung zum Internet.

Verwenden Sie nur sichere Verbindungen und Authentifizierungsmethoden für den Zugriff auf Unternehmensressourcen.

Home-Office

ARS DOCENDI ACADEMY

Systeme aktuell halten

Überprüfen Sie regelmäßig Ihre Sicherheitseinstellungen und halten Sie Ihr Betriebssystem und Ihre Software auf dem neuesten Stand. Installieren Sie Sicherheitspatches und Updates umgehend, um bekannte Sicherheitslücken zu schließen.

Home-Office

ARS DOCENDI ACADEMY

Sicherheitsbewusstsein schärfen!

Es ist wichtig, dass Sie sich der Sicherheitsrisiken bewusst sind, wenn Sie von zu Hause oder von unterwegs aus arbeiten.

Schärfen Sie Ihr Sicherheitsbewusstsein, indem Sie regelmäßig Schulungen und Sicherheitshinweise unseres Unternehmens durcharbeiten.

Home-Office

ARS DOCENDI ACADEMY

Vorsicht bei Mails

Seien Sie vorsichtig, wenn Sie E-Mails öffnen oder Links anklicken, und melden Sie verdächtige Aktivitäten oder E-Mails sofort dem IT-Team.

Home-Office

ARS DOCENDI ACADEMY

Sicheres Passwortmanagement

- Verwenden Sie für alle Ihre Konten nur sichere Passwörter und ändern Sie diese regelmäßig.
- Vermeiden Sie leicht zu erratende oder zu knackende Passwörter wie Geburtsdaten oder Namen von Familienmitgliedern.
- Generieren und speichern Sie stattdessen komplexe und einzigartige Passwörter mithilfe von Passwort-Managern.

Home-Office

ARS DOCENDI ACADEMY

Geräte nicht verleihen

Verbieten Sie Ihren Familienmitgliedern oder Mitbewohnern, Ihre Dienstgeräte zu benutzen, und benutzen Sie sie selbst nicht für private Zwecke.

Lassen Sie keine Passwörter offen herumliegen. Sperren Sie den Bildschirm, wenn Sie den Arbeitsplatz verlassen.

Home-Office

ARS DOCENDI ACADEMY

Sichere Speicherung von Daten

Legen Sie keine Unternehmensdaten auf ungesicherten Geräten oder bei Cloud-Speicheranbietern ab, die nicht von der IT-Abteilung autorisiert wurden.

Home-Office

ARS DOCENDI ACADEMY

Nur verschlüsselte Datenträger verwenden!

Verwenden Sie verschlüsselte Festplatten oder USB-Sticks, um sicherzustellen, dass sensible Daten bei Verlust oder Diebstahl geschützt sind.

Das gilt auch für interne Datenträger wie die Festplatten in Ihrem Laptop.

Home-Office

ARS DOCENDI ACADEMY

Datensparsamkeit

Löschen Sie auch regelmäßig Dateien, die Sie nicht mehr benötigen.

Home-Office

ARS DOCENDI ACADEMY

Nutzung von VPN

Wenn Sie außerhalb des Büros arbeiten, verwenden Sie ausschließlich ein Virtual Private Network (VPN), um sichere Verbindungen zum Internet und zu Unternehmensressourcen herzustellen.

Ein VPN verschlüsselt Ihren Datenverkehr. Es schützt Ihre Identität und Ihre Daten vor Hackern und anderen Bedrohungen.

Home-Office

ARS DOCENDI ACADEMY

Datensicherung

Sichern Sie Ihre Daten regelmäßig. So stellen Sie sicher, dass wichtige Informationen im Falle eines Datenverlusts wiederhergestellt werden können.

Speichern Sie Backups auf sicheren Geräten oder bei Anbietern von Cloud-Speicherdiensten, die von der IT-Abteilung als vertrauenswürdig eingestuft wurden.

Home-Office

ARS DOCENDI ACADEMY

Dokumente sicher austauschen

Verwenden Sie sichere Methoden, um Dokumente auszutauschen, und vermeiden Sie es, Daten über unsichere Netzwerke oder ungesicherte (Cloud-)Dienste auszutauschen.

Home-Office

ARS DOCENDI ACADEMY

Sicherheitsverletzungen oder -vorfälle melden

Wenn Sie bei der Arbeit von zu Hause oder von unterwegs auf eine mögliche Sicherheitsverletzung oder einen -vorfall aufmerksam werden, ist es wichtig, dass Sie den Vorfall umgehend melden.

Dies ermöglicht unserem Unternehmen, schnell und angemessen zu reagieren und weitere Schäden können vermieden werden.

Home-Office

ARS DOCENDI ACADEMY

Sicherheitssoftware & -tools verwenden

Sie sind verpflichtet, die zur Verfügung gestellte Sicherheitssoftware und -tools aktiv zu nutzen und auf dem neuesten Stand zu halten.

Dazu gehört, Antiviren- und Anti-Malware-Programme regelmäßig zu aktualisieren sowie Firewalls und andere Sicherheitsmechanismen zu aktivieren.

Home-Office

ARS DOCENDI ACADEMY

Geräte und Netzwerke absichern

Stellen Sie sicher, dass Ihre Geräte und Netzwerke vor Angriffen von außen geschützt sind. Blockieren Sie unerwünschte Netzwerkzugriffe mit einer Firewall.

Home-Office

ARS DOCENDI ACADEMY

F2A aktivieren

Verwenden Sie Zwei-Faktor-Authentifizierung, wann immer dies möglich ist. So können Sie sich zusätzlich absichern.

Home-Office

ARS DOCENDI ACADEMY

Vertraulichkeit gewährleisten

Verhindern Sie, dass Dritte (z. B. Familienmitglieder) Zugang zu dienstlichen Dokumenten mit vertraulichem Inhalt haben.

Bewahren Sie diese deshalb in einem verschlossenen Raum oder in einem verschlossenen Schrank auf.

Home-Office

ARS DOCENDI ACADEMY

Heimliche Lauscher abschalten

Schalten Sie Siri, Alexa und ähnliche Dienste während Telefonaten und Videokonferenzen aus. Die Mikrofone können Audio-Daten an den entsprechenden Anbieter übertragen.

Home-Office

ARS DOCENDI ACADEMY

Öffentlicher Netzwerke sicher nutzen

Stellen Sie bei der Nutzung öffentlicher Netzwerke sicher, dass diese verschlüsselt sind. Benutzen Sie dazu nur Netzwerke, die mit WPA2 oder höher verschlüsselt arbeiten.

Verwenden Sie für vertrauliche Informationen wie Passwörter oder Bankdaten keine öffentlichen WLAN-Netzwerke.

Home-Office

ARS DOCENDI ACADEMY

Verbindung beenden

Beenden Sie auch die Verbindung zum Firmennetzwerk und trennen Sie sich von öffentlichen Netzwerken, wenn Sie Ihre Arbeit beendet haben.

Schalten Sie Ihre Geräte aus oder sperren Sie sie. So verhindern Sie unbefugten Zugriff.

Home-Office

ARS DOCENDI ACADEMY

Daten und Geräte verantwortungsbewusst entsorgen

Sie müssen sicherstellen, dass alle Daten und Informationen auf Geräten oder Datenträgern, die nicht mehr benötigt oder ausgetauscht werden müssen, vollständig gelöscht oder vernichtet werden.

Dies gilt auch für Dokumente und Ausdrucke in Papierform. Damit vertrauliche Informationen nicht in falsche Hände geraten, sollten Daten nur auf sichere Weise entsorgt werden.

Home-Office