Bring your own device

Mitarbeiter, die ihr eigenes mobiles Gerät für die Arbeit verwenden dürfen, müssen einige wichtige Aspekte der Datensicherheit beachten. Hier sind einige Punkte, auf die sie besonders achten sollten!

ARS DOCENDI
ACADEMY

Geräteregistrierung

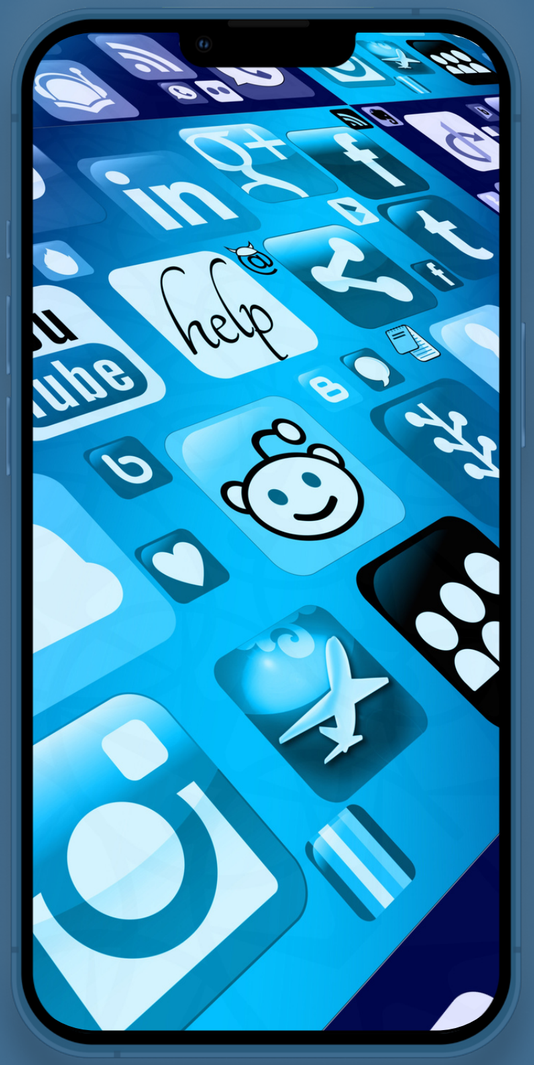
Alle persönlichen Geräte, die für Arbeitszwecke verwendet werden, müssen bei der IT-Abteilung des Unternehmens registriert werden. Dadurch wird sichergestellt, dass das Gerät mit den Sicherheitsrichtlinien des Unternehmens übereinstimmt und dass die erforderliche Software und Updates installiert sind.

ARS DOCENDI
ACADEMY

Passwortschutz

Der Zugriff auf das mobile Gerät sollte durch ein starkes Passwort oder eine biometrische Authentifizierung geschützt sein, um unbefugten Zugriff auf die gespeicherten Daten zu verhindern.

ARS DOCENDI
ACADEMY



Aktualisierte Software

Die Software des Geräts sollte immer auf dem neuesten Stand gehalten werden, um Schwachstellen und Sicherheitslücken zu minimieren. Das Betriebssystem muss also noch vom Hersteller aktiv unterstützt und mit Sicherheitspatches versorgt werden.

Antivirus-Software

Es ist empfehlenswert, eine Antivirus-Software auf dem mobilen Gerät zu installieren, um Schutz vor Malware und Viren zu gewährleisten.

Datenverschlüsselung

Sensible Daten sollten verschlüsselt gespeichert werden, um zu verhindern, dass sie im Falle eines Diebstahls oder Verlusts des Geräts in die falschen Hände geraten.

ARS DOCENDI
ACADEMY

Einschränkung von App-Berechtigungen

Es ist wichtig, die Berechtigungen von Apps, die auf dem Gerät installiert sind, zu überprüfen und einzuschränken, um sicherzustellen, dass sie nicht auf sensible Daten zugreifen können.

ARS DOCENDI ACADEMY

Netzwerksicherheit

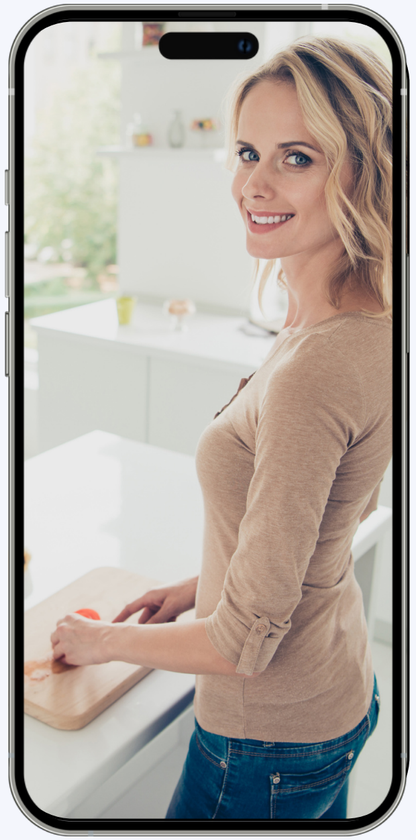
Mitarbeiter sollten bei der Nutzung ihres mobilen Geräts für die Arbeit öffentliche WLAN-Netzwerke meiden, da diese unsicher sein können und Daten abgefangen werden könnten. Stattdessen sollten sie ein sicheres Netzwerk nutzen oder eine VPN-Verbindung herstellen.

Sicherheitsrichtlinien

Mitarbeiter müssen sich mit den Sicherheitsrichtlinien ihres Arbeitgebers vertraut machen und sicherstellen, dass sie diese einhalten, um das Risiko von Sicherheitsverletzungen zu minimieren.

ARS DOCENDI
ACADEMY

Trennung von persönlichen und beruflichen Daten:



Persönliche und arbeitsbezogene Daten müssen auf dem Gerät getrennt gehalten werden. Dies kann durch die Verwendung getrennter Benutzerkonten erreicht werden.

Meldung verlorener oder gestohlener Geräte.

Mitarbeitende müssen verlorene oder gestohlene Geräte unverzüglich der IT-Abteilung des Unternehmens melden, damit diese alle notwendigen Maßnahmen ergreifen kann, wie z. B. die Löschung der Daten von dem Gerät aus der Ferne.

ARS DOCENDI ACADEMY

Lassen Sie NIE Ihr Gerät unbeaufsichtigt!

ARS DOCENDI ACADEMY

Angemessene Nutzung

Während der Arbeitszeit dürfen die Mitarbeiter ihre persönlichen Geräte nur für berufliche Zwecke und nicht für private Aktivitäten verwenden.

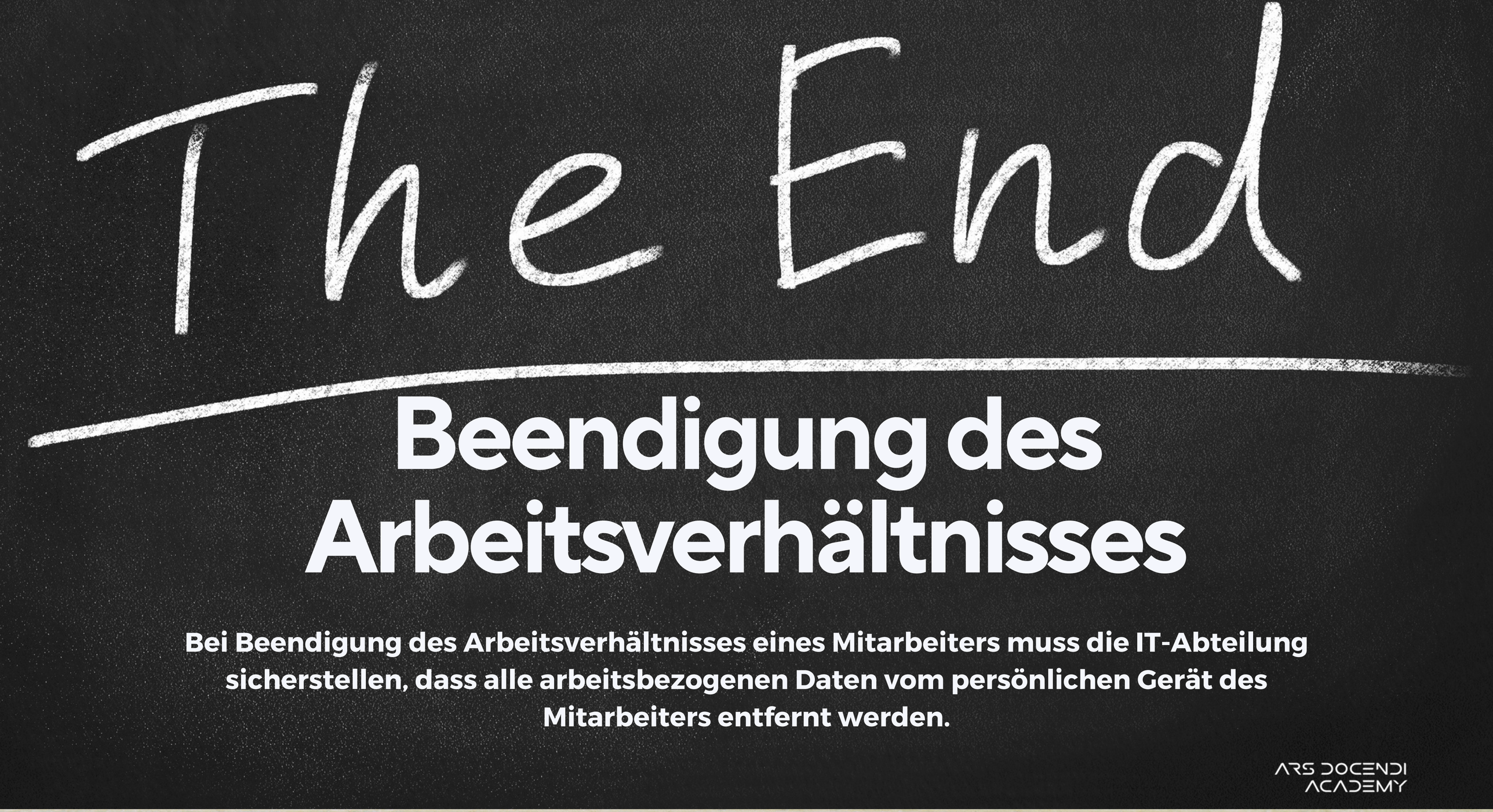
ARS DOCENDI ACADEMY

Fernzugriff

Alle Mitarbeitenden müssen sichere Methoden wie VPNs verwenden, wenn sie von ihren persönlichen Geräten aus auf Unternehmensressourcen zuzugreifen, z. B. von unterwegs oder aus dem Home-Office.

Einhaltung von Gesetzen und Vorschriften

Selbstverständlich müssen unsere Mitarbeiter alle geltenden Gesetze und Vorschriften einhalten, z. B. Die DSGVO oder Gesetze zum Schutz der Privatsphäre, wenn sie ihre persönlichen Geräte für Arbeitszwecke verwenden.



Beendigung des Arbeitsverhältnisses

Bei Beendigung des Arbeitsverhältnisses eines Mitarbeiters muss die IT-Abteilung sicherstellen, dass alle arbeitsbezogenen Daten vom persönlichen Gerät des Mitarbeiters entfernt werden.

ARS DOCENDI ACADEMY

Zulässige Geräte

Das Unternehmen kann eine Liste zulässiger Geräte erstellen, die für Arbeitszwecke verwendet werden dürfen. Diese Geräte sollten den Mindestsicherheitsanforderungen entsprechen und müssen bei der IT-Abteilung registriert werden.