Inhaltsverzeichnis

Arbeitsanweisungen

Neue Arbeitsanweisung erstellen oder eine bestehende bearbeiten:

Erstellen

Seitentitel	Geltungsbereich	VerisonAnzahl der freigegebenen Versionen in der Versionsgeschichte der Seite
Policy für die Nutzung mobiler Endgeräte	Unternehmensweit	4

Attribut:QM Coverage

This is a property of type Text.

Annotationen4
vorherige 202050100250500nächste 20

Filter
Unterhalb werden 4 Seiten angezeigt, auf denen für dieses Attribut ein Datenwert gespeichert wurde.
E
Erstellung eines Angebots +
Vertrieb +
K
Konformitätsprüfung der Compliance-Anforderungen der Abteilung IT-Services +
IT Services +
Korrekturmaßnahmen +
Unternehmensweit +
P
Policy für die Nutzung mobiler Endgeräte +
Unternehmensweit +

Attribut:QM/Dokumentenversion (QM/Document version)

Anzahl der freigegebenen Versionen in der Versionsgeschichte der Seite Dieses Attribut ist softwareseitig fest definiert und auch bekannt als Spezialattribut. Es erfüllt eine besondere Funktion, kann aber wie jedes andere benutzerdefinierte Attribut verwendet werden.
Annotationen81
vorherige 202050100250500nächste 20

Filter
Unterhalb werden 20 Seiten angezeigt, auf denen für dieses Attribut ein Datenwert gespeichert wurde.
1
127.0.0.1 +
0 +
2
24.134.101.133 +
0 +
8
82.135.30.117 +
0 +
A
Ablauforganisation +
2 +
Administratorenportal +
0 +
Arbeitsanweisungen +
2 +
Audits +
1 +
Aufbauorganisation +
4 +
B
Benutzer anlegen +
0 +
C
CHECKLIST +
0 +
CUSER +
0 +
D
Der Demingkreis - Handeln +
1 +
Der Demingkreis - Planen +
2 +
Der Demingkreis - Umsetzen +
1 +
Der Demingkreis - Überprüfen +

1 +
E
ERRC +
0 +
ERRT +
0 +
EUSER +
0 +
EXIFCOLORSPACE +
0 +
EXIFDATETIME +
0 +

QM:Policy für die Nutzung mobiler Endgeräte

Der Einsatz mobiler IT-Geräte (Notebooks, Smartphones, Tablet-PCs) birgt erhebliche Gefahren für das Unternehmen: Vertrauliche Unternehmensdaten werden außerhalb des Unternehmens gespeichert und verwendet. Portable Geräte sind für Diebe eine attraktive, leicht zu verkaufende Beute.

Arbeitsanweisung	
Anweisungen zur Nutzung mobiler IT-Geräte durch Mitarbeiter.	
Geltungsbereich	Unternehmensweit
Version	4

Wenn Sie mobile IT-Geräte benutzen, sind die folgenden Regelungen zu beachten.

Inhaltsverzeichnis

Zulassung und Genehmigung

- Falls Sie Ihr eigenes Smartphone oder Tablet für berufliche Zwecke einsetzen wollen: Klären Sie zuvor mit Ihren IT-Zuständigen und Vorgesetzten ab, ob diese Verwendung in Ihrem Unternehmen zugelassen ist. Stellen Sie gemeinsam sicher, dass alle notwendigen Sicherheitsmaßnahmen umgesetzt wurden!
- Falls Ihr Unternehmen eine Mobile Device Management-Lösung einsetzt: Verwenden Sie für berufliche Zwecke ausschließlich die dafür vorgesehenen Anwendungen und verarbeiten Sie keine dienstlichen Daten im privaten, ungeschützten Bereich!

Diebstahlsichere Aufbewahrung und Verhalten bei Diebstahl

- Sorgen Sie für eine diebstahlsichere Aufbewahrung Ihres Gerätes. Bewahren Sie es grundsätzlich nicht im Fahrzeug auf. Ist dies nicht zu vermeiden, decken Sie das Gerät ab oder schließen Sie es im Kofferraum ein.
- Lassen Sie das Gerät nicht unbeaufsichtigt und überlassen Sie es nicht anderen Personen! Sperren Sie es bei kurzen Arbeitspausen oder schalten Sie es ab. Stellen Sie es so ein, dass es nur nach Überwinden einer Zugriffschutzfunktion (Passwort, PIN, Fingerprint, Erkennungsmuster, ...) bedient werden kann.
- Melden Sie einen Diebstahl oder Verlust sofort der IT-Abteilung! Möglicherweise müssen Fernzugänge zu Ihrem Unternehmen gesperrt oder Passwörter geändert werden, um unerlaubte Zugriffe zu unterbinden. Die rasche Meldung des Vorfalls kann helfen, weitere Sicherheitsverstöße zu verhindern.

Einsatz von Schutzprogrammen und Installation von Apps

- Es gibt verschiedene Programme und Dienste, die es erlauben, alle Daten auf einem gestohlenen oder verlorenen Smartphone aus der Distanz zu löschen. Setzen Sie diese Apps unbedingt ein! Auch der Einsatz von Virenschutzprogrammen für Smartphones und Tablets ist dringend anzuraten.
- Verschlüsseln Sie die Festplatteninhalte bzw. wichtige Dateien und verhindern Sie damit unbefugten Zugriff auf Firmendaten. Aktivieren Sie auch auf Ihrem Smartphone oder Tablet die Dateiverschlüsselung oder setzen Sie eine Verschlüsselungs-App zum Speichern sensibler Daten ein!
- Installieren Sie nur Apps, die Ihnen als vertrauenswürdig und sicher bekannt sind! Fragen Sie im Zweifelsfall Ihre IT-Zuständigen oder recherchieren Sie im Internet, ob dazu Gefahren bekannt sind.
- Viele Apps verlangen bei der Installation Zugriff auf verschiedenste Gerätefunktionen (WLAN, GPS-Empfänger...). Überlegen Sie selbst, ob es nötig ist, dass z.B. eine Spiele-App Zugriff auf Ihr Mikrophon oder Ihr Adressbuch erhält. Installieren Sie nur Apps, deren Zugriffsanforderungen Sie für vertrauenswürdig halten!

Nutzung öffentlicher Netzwerke und Cloudservices

- Vermeiden Sie kostenlose, öffentlich zugängliche WLAN-Netzwerke, wenn Sie Mobilgeräte für berufliche Zwecke einsetzen: Ihre unverschlüsselte Kommunikation über das Netzwerk kann problemlos abgehört werden. Im schlimmsten Fall können auch Daten auf Ihrem Gerät ausgelesen werden.
- Sorgen Sie für Sichtschutz, wenn Sie das Gerät in der Öffentlichkeit verwenden (z.B. am Flughafen) – das verhindert das Ausspähen von Unternehmensinformationen.
- Verwenden Sie Ihren privaten Cloud-Speicherdienst (Dropbox, iCloud, Google Drive) nicht für Unternehmensdaten! Fragen Sie bei Ihren IT-Zuständigen nach, welche Möglichkeiten bestehen, um Firmendokumente über das Internet sicher abzuspeichern.

Abschaltregeln

- Deaktivieren Sie alle nicht gerade benötigten Geräteschnittstellen (USB, WLAN, Infrarot, Bluetooth). Wenn diese Schnittstellen (z.B. WLAN für Internetverbindung) unbedingt notwendig sind, müssen entsprechende Schutzmaßnahmen (Personal Firewall, aktuelles Virenschutzprogramm usw.) vorgesehen werden.
- Schalten Sie den GPS-Empfänger auf Ihrem Smartphone immer ab, wenn er nicht gebraucht wird.
- Auf Smartphones oder Tablets, die Sie für berufliche Zwecke verwenden, dürfen Sie nie interne Sicherheitsmechanismen außer Kraft setzen (z.B. „Jailbreaks“ oder “Rooten“)! Durch diese Manipulationen entstehen zusätzliche Gefahrenquellen für die gespeicherten Unternehmensdaten.
- Lassen Sie Ihr Smartphone bei vertraulichen Besprechungen an Ihrem Arbeitsplatz oder schalten Sie es in den Flugmodus!

Entsorgung

- Bevor Sie ein Smartphone verkaufen, weitergeben oder entsorgen, müssen Sie sicherstellen, dass alle gespeicherten Daten gelöscht wurden. Am besten eignet sich dazu ein „Factory Reset“. Danach müssen Sie überprüfen, ob noch Einstellungen oder Daten erhalten geblieben sind.