SOCIAL MEDIA

RICHTLINIE

Version 1.0 • 08/2023

Richtlinie zur Nutzung von Social Media unter dem Aspekt der Cyber-Sicherheit

In dieser Richtlinie wird die Nutzung von Social Media unter dem Aspekt der Cyber-Sicherheit behandelt. Zur Nutzung von Social Media unter inhaltlichen und formalen Aspekten beachten Sie bitte auch die Social Media-Richtlinie 01.

Einleitung

Diese Richtlinie legt zur Gewährleistung der Sicherheit von Unternehmensinformationen und zur Minimierung von Cyber-Bedrohungen die Anforderungen und Best Practices für die Nutzung von Social Media durch Mitarbeiterinnen und Mitarbeiter fest.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter, die Social Media nutzen. Dies kann sowohl für berufliche als auch für private Zwecke geschehen, während sie Zugang zu Unternehmensressourcen haben.Grundlegende Anforderungen

Bewusstsein schaffen

Unsere Mitarbeiterinnen und Mitarbeiter müssen sich der Risiken im Umgang mit Social Media bewusst sein. Sie werden regelmäßig geschult.

RICHTLINIE

Trennung von Privatem und Geschäftlichem

Die strikte Trennung von privaten und geschäftlichen Social Media Accounts ist für alle Mitarbeiterinnen und Mitarbeiter verpflichtend.

Starke Passwörter

Für alle Social-Media-Accounts müssen starke und eindeutige Passwörter verwendet werden. Dabei kann die Verwendung von Passwort-Managern helfen. In der Passwort-Richtlinie finden Sie Vorschriften für sichere Passwörter.

Best Practices

Zugriffsbeschränkungen

Verwenden Sie die strengsten Datenschutzeinstellungen für Ihre Konten und überprüfen Sie diese Einstellungen in regelmäßigen Abständen.

Vorsicht bei Links

Folgen Sie nicht leichtfertig Links oder laden Sie keine Dateien von unbekannten Quellen herunter.

Phishing-Betrug

Seien Sie vorsichtig bei Nachrichten, in denen persönliche Informationen oder Anmeldedaten verlangt werden.

Vertraulichkeit wahren

Der Austausch vertraulicher oder geschäftskritischer Informationen über soziale Medien ist verboten.

Zwei-Faktor-Authentifizierung

Aktivieren Sie die Zwei-Faktor-Authentifizierung für Ihre Konten, wo immer dies möglich ist.

Umgang mit Vorfällen

Sicherheitsvorfälle melden

Informieren Sie sofort das IT-Team, wenn Sie vermuten, dass Ihr Konto kompromittiert wurde.

Konto wiederherstellen

Befolgen Sie zur Wiederherstellung des Zugriffs auf Ihr Konto die Anweisungen des IT-Teams oder des Social-Media-Anbieters.

Nutzung von Unternehmensgeräten

Eingeschränkte Nutzung:

Die Nutzung von Social Media auf Unternehmensgeräten muss auf das absolut Notwendige beschränkt werden, es sei denn, sie wird für Ihre berufliche Tätigkeit benötigt.

Apps und Software

Laden Sie ohne vorherige Genehmigung der IT-Abteilung keine Social-Media-Anwendungen oder sonstige Software auf Unternehmensgeräte herunter.

Vorsicht bei Freundschaftsanfragen und Nachrichten

Unbekannte Anfragen

Seien Sie vorsichtig im Umgang mit Freundschaftsanfragen von Personen, die Sie nicht kennen, insbesondere wenn diese Personen behaupten, mit unserem Unternehmen in Verbindung zu stehen.

Verdächtige Nachrichten

Ignorieren Sie Nachrichten von unbekannten Absendern und melden Sie diese, vor allem, wenn Sie darin nach persönlichen Informationen oder Log-In-Daten gefragt werden.

Informationen weitergeben

Keine Arbeitsdetails weitergeben

Es ist verboten, spezifische Arbeitsdetails, Zeitpläne oder interne Prozesse auszutauschen.

Vorsicht mit Bildern

Es ist verboten, Bilder zu posten, die sensible Informationen wie Firmendokumente, Computerbildschirme oder Sicherheitsausweise zeigen.

Ohne vorherige Genehmigung der Abgebildeten ist es nicht gestattet, Fotos von Mitarbeitenden, Kunden oder anderen Personen, die mit unserem Unternehmen verbunden sind, zu posten. Im Zweifelsfall müssen Sie den Nachweis für dre erteilte Genehmigung erbringen.

Schulungen und Workshops

Regelmäßige Schulungen:

Mitarbeiterinnen und Mitarbeiter sollten regelmäßig an Cyber-Sicherheitsschulungen teilnehmen. Dazu gehört auch der sichere Umgang mit Social Media.

Aktuelle Bedrohungen:

Die Mitarbeitenden werden von der IT-Abteilung über aktuelle Bedrohungen oder Phishing-Kampagnen, die über Social Media verbreitet werden, informiert.

Überwachung und Compliance

Überwachung

Um die Einhaltung dieser Richtlinie sicherzustellen, behält sich das Unternehmen das Recht vor, die Nutzung von Social Media auf Firmengeräten zu überwachen.

Durchsetzung

Verstöße gegen diese Richtlinie können disziplinarische Maßnahmen bis hin zur Kündigung zur Folge haben.

Schlussbestimmungen

Überprüfung und Aktualisierung

Diese Richtlinie wird zur Anpassung an die sich verändernde Cyber-Sicherheitslandschaft regelmäßig überprüft und aktualisiert.

RICHTLINIE

Nichteinhaltung

Verstöße gegen diese Richtlinie können disziplinarische Maßnahmen nach sich ziehen, einschließlich - aber nicht beschränkt auf - den Entzug des Zugriffs auf die Ressourcen des Unternehmens.

Zustimmung

Durch die Nutzung von Social Media im Kontext des Zugriffs auf Unternehmensressourcen erklären sich die Mitarbeiterinnen und Mitarbeiter mit den Bestimmungen dieser Richtlinie einverstanden und sind verpflichtet, diese einzuhalten.

Diese Richtlinie ist ein Leitfaden für die sichere Nutzung von Social Media und soll zur Schärfung des Bewusstseins für Cyber-Sicherheitsrisiken beitragen. Sich sicher und verantwortungsvoll in der digitalen Welt zu bewegen, liegt in der Verantwortung jedes Einzelnen.

RICHTLINIE