

Richtlinie für mobile Geräte

INGOLD SOLUTIONS GMBH

Richtlinie für mobile Geräte
(Referenz-Nr.: ISMS/IS/5.2/01)

Zweck:

Diese Richtlinie beschreibt die Nutzung mobiler Geräte durch Mitarbeiter von INGOLD SOLUTIONS GMBH.

Sie ist von allen Mitarbeitern zu lesen und zu verstehen, die:

- Ein unternehmenseigenes mobiles Gerät nutzen
- Ein persönliches mobiles Gerät auf das Firmengelände bringen

Richtlinie:

Nutzung persönlicher mobiler Geräte:

Mitarbeiter dürfen persönliche Geräte für Arbeitszwecke nur nach vorheriger schriftlicher Genehmigung durch sich selbst und die Geschäftsleitung verwenden. Persönliche elektronische Geräte umfassen u. a. private Handys, Tablets, Laptops und Computer.

Ohne schriftliche Genehmigung und Zustimmung dürfen persönliche Geräte nicht für Arbeitszwecke genutzt werden. Verstöße können disziplinarische Maßnahmen bis hin zur Kündigung zur Folge haben.

Nutzung unternehmenseigener mobiler Geräte:

Bestimmte Mitarbeiter erhalten je nach Aufgabenbereich ein unternehmenseigenes mobiles Gerät. Dieses bleibt Eigentum von INGOLD SOLUTIONS GMBH.

Sicherheit:

Jedes Gerät, das auf Unternehmensdaten zugreift, muss mit PIN, Passwort oder ähnlichen Schutzmaßnahmen gesichert sein. Zusätzlich ist MDM-Software (Mobile Device Management) auf persönlichen Geräten erforderlich, wie von PDS INFOTECH empfohlen. Die Installation erfolgt durch die IT-Abteilung.

Zwei-Faktor-Authentifizierung ist nach Möglichkeit zu verwenden.

Cloud-Apps oder Backups, die Unternehmensdaten unsicheren Dritten zugänglich machen, sind nicht erlaubt. Geräte dürfen nicht mit Heimgeräten synchronisiert werden. Unautorisierte Hardware-/Softwareänderungen sind verboten. Unsichere Internetseiten dürfen nicht genutzt werden.

Kameras, Video- oder Aufnahmefunktionen persönlicher Geräte dürfen ohne vorherige Genehmigung nicht auf dem Firmengelände genutzt werden.

Daten früherer Arbeitgeber dürfen nicht auf unternehmenseigenen Geräten gespeichert werden.

Verhalten:

Während der Arbeit ist beim Gebrauch privater Geräte dieselbe Sorgfalt wie bei Firmengeräten anzuwenden. Unternehmensrichtlinien zu Belästigung, Diskriminierung, Geheimhaltung usw. gelten auch für private Geräte bei dienstlicher Nutzung.

Exzessive private Kommunikation während der Arbeitszeit stört und ist zu vermeiden. Private Angelegenheiten sind in Pausen zu klären. Ausnahmen gelten nur im Notfall oder mit Genehmigung.

Während Meetings oder Konferenzen sind mobile Geräte stumm oder im Vibrationsmodus zu halten.

Arbeitszeiten:

Nicht freigestellte Mitarbeiter dürfen Geräte außerhalb der regulären Arbeitszeiten nur mit Genehmigung nutzen – z. B. für E-Mails, Anrufe oder Nachrichten.

Während unbezahltem Urlaub ist die Nutzung untersagt. Der Zugriff auf Unternehmensanwendungen kann deaktiviert werden.

Datenschutz:

Es besteht kein Anspruch auf Privatsphäre außer gesetzlich vorgeschrieben. Das Unternehmen darf alle über sein Netzwerk laufenden Kommunikationen überwachen, unabhängig vom Geräteeigentum. Es dürfen auch Daten an Behörden oder Dritte weitergegeben werden.

Mitarbeiter dürfen keine Überwachungssoftware deaktivieren.

Inspektion:

Das Unternehmen kann jederzeit die Vorlage des mobilen Geräts verlangen, um die Einhaltung der Richtlinie zu prüfen.

Sicherheit:

Alle gesetzlichen Vorschriften zur Nutzung elektronischer Geräte sind einzuhalten.

Bei Fahrten ist die Nutzung von Mobilgeräten untersagt, es sei denn, dies erfolgt vollständig freihändig. Bei schlechtem Wetter, Verkehr oder unbekannter Umgebung ist besondere Vorsicht geboten.

Verkehrsverstöße aufgrund der Gerätenutzung liegen in der Verantwortung des Mitarbeiters. In Gefahrenbereichen ist die Nutzung untersagt.

Verlust, Diebstahl, Hacking oder Beschädigung:

Geräte sind gegen Verlust oder Schaden zu schützen. MDM-Software mit Fernlöschfunktion ist Pflicht. Diese wird durch die IT installiert.

Im Verlustfall wird das Gerät per Fernzugriff auf Werkseinstellungen zurückgesetzt. Das Unternehmen haftet nicht für Datenverluste.

Bei Beschädigung ist dies sofort zu melden. Kosten trägt der Mitarbeiter. Vorsätzliche Schäden können zur Kündigung führen.

Beendigung des Arbeitsverhältnisses:

Nach Kündigung oder Austritt erfolgt eine Rücksetzung des Geräts mittels Fernlöschung. Das Unternehmen übernimmt keine Haftung für private Datenverluste.