

Sicherheitsanforderung

Fremdfirmen

Deutsche Telekom Gruppe

Version	2.1
Datum	01.07.2021
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.11	Dokumententyp Sicherheitsanforderung
Version 2.1	Stand 01.07.2021	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2021 - 30.06.2026	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung
Fremdfirmen

Copyright © 2021 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Organisatorische Maßnahmen	5

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt.

Die Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden. Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

Dieses Dokument ist nur anzuwenden, wenn der (Rahmen-)Vertrag mit der Fremdfirma *keinen* standardisierten Security Annex enthält.

2. Organisatorische Maßnahmen

Req 1	Erbringen Fremdfirmen Dienstleistungen, müssen die Auftraggeber die für die IT-/NT-Systeme erforderlichen Datenschutz- und Sicherheitsanforderungen über vertragliche Vereinbarungen mit der Fremdfirma festlegen und steuern.
-------	--

Der Auftraggeber ist als zentraler Ansprechpartner für das Thema Sicherheit auf DTAG Seite für die Verwaltung der Fremdfirma in diesem Kontext verantwortlich.

Motivation: Nur eine verbindliche vertragliche Vereinbarung stellt sicher, dass Fremdfirmen die Datenschutz- und Sicherheitsanforderungen umsetzen.

ID: 3.11-1/2.1

Req 2	Die Fremdfirma muss über einen technischen und organisatorischen Identitätsmanagementprozess verfügen, mit dem die Identitäten der Nutzer mit Zugang zu Systemen der Deutschen Telekom Gruppe verwaltet werden.
-------	---

Der Identitätsmanagementprozess muss eingeführt und nachvollziehbar dokumentiert sein. Informationen über diesen Prozess muss die Fremdfirma auf Anfrage der Deutschen Telekom Gruppe umgehend bereitstellen können. Die Zuweisung von Identitäten muss dem Berechtigungskonzept folgen, das die Deutsche Telekom Gruppe bereitstellt.

Motivation: Ein angemessener Identitätsmanagementprozess reduziert die Risiken der Abstreitbarkeit von Handlungen oder Missbrauch.

ID: 3.11-2/2.1

Req 3	Die Fremdfirma muss in der Lage sein, der Deutschen Telekom Gruppe jederzeit detaillierte Informationen (einschließlich Berechtigungen) über die zugewiesenen Nutzer bereitzustellen.
-------	---

Motivation: Auf diese Weise lässt sich die angemessene Handhabung des Need-to-know- und Need-to-do- Prinzips verifizieren und verfolgen.

ID: 3.11-3/2.1

Req 4	Die Fremdfirma muss ein aktuelles Security Framework umsetzen und dieses auf Nachfrage der Deutsche Telekom Gruppe vorlegen.
-------	--

Der Begriff Framework umfasst mindestens die Blöcke

- Definition Sicherheitsprozesse
- Definition Sicherheitsvorgaben

Motivation: Die Umsetzung eines Security Frameworks stellt eine strukturierte und nachvollziehbare Herangehensweise in Sicherheitsfragen sicher.

ID: 3.11-4/2.1

Req 5	Die Fremdfirma muss ihre Mitarbeiter im Zusammenhang mit dem Security Framework ihres Unternehmens angemessen und regelmäßig ausbilden.
-------	---

Die Fremdfirma muss sicherstellen, dass die autorisierten Nutzer, die im Zusammenhang des Auftrages Zugang zu IT-Anlagen und IT-Einrichtungen der Deutsche Telekom Gruppe erhalten, angemessen für die effiziente Nutzung dieser Einrichtungen ausgebildet worden sind.

Motivation: Schulungen im Sicherheitsbewusstsein sind eine weitere Voraussetzung für die erfolgreiche Umsetzung des Security Frameworks.

ID: 3.11-5/2.1

Req 6	Die Fremdfirma muss einen Sicherheitsbeauftragten benennen, der im Zusammenhang mit allen Anliegen auf dem Gebiet der Informationssicherheit der Ansprechpartner für die Deutsche Telekom Gruppe ist.
-------	---

Motivation: Ein zentraler Ansprechpartner und eindeutig geregelte Zuständigkeiten sind eine Voraussetzung für eine rasche und effiziente Problemlösung bei möglichen Vorfällen.

ID: 3.11-6/2.1

Req 7	Die Fremdfirma muss sicherstellen, dass sie Sicherheitsvorfälle sofort nach deren Feststellung den ihr gegenüber benannten Sicherheitsbeauftragten der Deutschen Telekom Gruppe meldet. Dies gilt für alle Vorfälle, die den für die Deutsche Telekom Gruppe bereitgestellten Dienst betreffen beziehungsweise diesen beeinträchtigen könnten.
-------	--

Motivation: Die Fremdfirma muss die Deutsche Telekom Gruppe auf dem neuesten Informationsstand halten, damit die Telekom auf Sicherheitsvorfälle reagieren kann.

ID: 3.11-7/2.1

Req 8	Die Deutsche Telekom Gruppe muss die Fremdfirma an einen Geheimhaltungsvertrag beziehungsweise eine ähnliche vertragliche Vereinbarung binden.
-------	--

Motivation: Ein solcher Vertrag hat das Ziel, für klar geregelte juristische Verhältnisse zu sorgen.

ID: 3.11-8/2.1

Req 9	Beabsichtigt eine Fremdfirma, die der Deutschen Telekom Gruppe bereitgestellten Dienstleistungen beziehungsweise Teile davon vertraglich an einen Unterauftragnehmer zu vergeben, muss das Unternehmen vorher eine schriftliche Erlaubnis von der Deutschen Telekom Gruppe einholen.
-------	--

Motivation: Unterverträge zwischen einem Dritten und Vierten dürfen keine negativen (sicherheitsbezogenen) Auswirkungen auf die Deutsche Telekom Gruppe haben.

ID: 3.11-9/2.1

Req 10	Die Fremdfirma muss sicherstellen, dass alle Sicherheitsanforderungen des von ihr bereitgestellten Dienstes auch für ihre Unterauftragnehmer gelten.
--------	--

Motivation: Unterverträge zwischen einem Dritten und Vierten dürfen keine negativen (sicherheitsbezogenen) Auswirkungen auf die Deutsche Telekom Gruppe haben.

ID: 3.11-10/2.1

Req 11	Die Fremdfirma muss eine physische Sicherheitsrichtlinie erlassen und befolgen.
--------	---

Die Richtlinie muss Aspekte wie Gebäudesicherheit, Perimetersicherheit oder physische Zugangskontrolle regeln. Insbesondere Client-Einrichtungen, die die Fremdfirma zur Anbindung an die Deutsche Telekom Gruppe nutzt, muss das

Unternehmen über Zugangskontrollen angemessen absichern.

Motivation: Bedrohungen, die auf physischen Zugang zurückzuführen sind, muss die Fremdfirma auf der Basis einer geeigneten Richtlinie kontrollieren.

ID: 3.11-11/2.1

Req 12	Vertrauliche Daten, die der Deutschen Telekom Gruppe gehören, darf die Fremdfirma nicht ohne den Anforderungen der DTAG entsprechende, zusätzliche Schutzmechanismen lokal speichern.
--------	---

Mitunter ist wegen des Servicemodells eine lokale Speicherung erforderlich. In einem solchen Fall muss die Fremdfirma die Informationen in Übereinstimmung mit den Standards der Deutsche Telekom Gruppe verschlüsseln oder auf andere Weise angemessen vor unbefugtem Zugriff oder Missbrauch schützen. Die Handhabung der vertraulichen Daten muss den Informationsschutzrichtlinien und Datenschutzanforderungen der Deutschen Telekom Gruppe entsprechen. Die Fremdfirma muss ein Datenschutz- und Sicherheitskonzept erstellen.

ID: 3.11-12/2.1