Security requirement

Third Parties

Deutsche Telekom Group

Version	2.1
Date	Jul 1, 2021
Status	Released

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	3.11	Security requirement

Version	State	Status
2.1	Jul 1, 2021	Released

Contact	Validity	Released by
Telekom Security psa.telekom.de	Jul 1, 2021 - Jun 30, 2026	Stefan Pütz, Leiter SEC-T-TST

Summary
Third Parties

Table of Contents

1. Introduction

This security document has been prepared based on the general security policies of the Group.
The security requirement is used as a basis for an approval in the PSA process, among other things. It also serves as an implementation standard for units which do not participate in the PSA process. These requirements shall be taken into account from the very beginning, including during the planning and decision-making processes. When implementing these security requirements, the precedence of national, international and supranational law shall be observed.
This document is only applicable if the contractual (frame-)agreement with the 3rd party does *not* contain the standardised security annex.

2. Organizational requirements

Req 1	In the event that services are provided by third parties, internal customers must specify and manage the necessary data protection and security requirements for the IT/NT systems by entering into contractual agreements with the third-party providers.

The internal customer is the single point of contact for security at DTAG and therefore accountable for the management of the third party in this context.

Motivation: Entering into a binding contractual agreement is the only way to ensure that third-party providers fulfill the data protection and security requirements.

ID: 3.11-1/2.1

Req 2	Every third-party provider must have a technical and organizational identity management process in place, which is used for administration of the identities of users who have access to systems operated by the Deutsche Telekom Group.

The identity management process must be introduced and documented transparently. The third-party provider must be able to provide the Deutsche Telekom Group with information about this process on request. Assignment of identities must follow the authorization concept that the Deutsche Telekom Group makes available.

Motivation: An appropriate identity management process reduces the risk of deniability of actions or misuse.

ID: 3.11-2/2.1

Req 3	Every third-party provider muss be in a position to provide the Deutsche Telekom Group with detailed information (including authorizations) about the assigned users at any time.

Motivation: This makes it possible to verify and monitor appropriate application of the need-to-know and need-to-do principles.

ID: 3.11-3/2.1

Req 4	The third-party provider must implement a state-of-the-art security framework and present this to the Deutsche Telekom Group on request.

The term framework covers at least the following blocks:

- Definition of security processes and
- Definition of security requirements

Motivation: The implementation of a security framework guarantees a structured and transparent approach with regard to security matters.

ID: 3.11-4/2.1

Req 5	Every third-party provider must provide its employees with appropriate regular training in conjunction with the company's security framework.

Third-party providers must ensure that authorized users who are granted access to IT systems and IT equipment of the Deutsche Telekom Group in conjunction with the commissioning of a specific order are given appropriate training to enable them to use these facilities efficiently.

Motivation: Training in security awareness is a further prerequisite for successful implementation of the security framework.

ID: 3.11-5/2.1

Req 6	Third-party providers must name a security officer to act as contact with the Deutsche Telekom Group in all matters relating to information security.

Motivation: A central contact and clearly defined responsibilities are prerequisites for prompt and efficient problem resolution if and when an incident occurs.

ID: 3.11-6/2.1

Req 7	Every third-party provider must ensure that security incidents are reported to the security officer of the Deutsche Telekom Group named to it immediately on discovery. This applies to all incidents that affect the service provided for the Deutsche Telekom Group or that could compromise it.

Motivation: The Third-party provider shall keep the Deutsche Telekom Group informed about the latest occurrences, so that Telekom is in a position to react to security incidents.

ID: 3.11-7/2.1

Req 8	The Deutsche Telekom Group must oblige the third-party provider to sign a binding non-disclosure agreement or similar contractual agreement.

Motivation: The object of an agreement of this nature is to ensure that clear legal conditions prevail.

ID: 3.11-8/2.1

Req 9	If third-party providers plan to contract out services or parts of services for the Deutsche Telekom Group to a subcontractor, they must obtain prior written consent from the Deutsche Telekom Group.

Motivation: Subcontracts between third and fourth parties shall not have a negative (security-related) impact on the Deutsche Telekom Group.

ID: 3.11-9/2.1

Req 10	Every third-party provider must ensure that all security requirements which apply to the services it provides are also valid for any subcontractors.

Motivation: Subcontracts between third and fourth parties shall not have a negative (security-related) impact on the Deutsche Telekom Group.

ID: 3.11-10/2.1

Req 11	The third-party provider must issue and comply with a physical security policy.

The policy must govern aspects such as building security, perimeter security and physical access control. In particular, client equipment which a third party provider uses to connect to the Deutsche Telekom Group must provide the Company with suitable protection through access controls.

Motivation: Third-party providers shall control threats relating to physical access with an appropriate policy.

ID: 3.11-11/2.1

Req 12	The third-party provider must not store confidential data belonging to the Deutsche Telekom Group on local systems without additional protection mechanisms, compliant with DTAG internal policies.

The service model may sometimes make it necessary to store data locally. In such cases, third-party providers must encrypt the information in compliance with Deutsche Telekom Group standards, or use another method to protect it suitably from unauthorized access or misuse. Handling of confidential data must comply with the Deutsche Telekom Group's Policy on Information Security and Data Protection. Third-party providers must draw up a data protection and security concept.

ID: 3.11-12/2.1