Security requirement

External Hosting

Deutsche Telekom Group

Version	2.7
Date	Dec 1, 2023
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
	3.08	Security requirement

Version	State	Status
2.7	Dec 1, 2023	Released

Contact	Validity	Released by
Telekom Security psa.telekom.de	Dec 1, 2023 - Nov 30, 2028	Stefan Pütz, Leiter SEC-T-TST

Summary
External Hosting

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.

2. Requirements for external security management

Req 1	The hosting provider must provide a policy-level contact for all security matters.

The contact should also be the interface for reports from the vulnerability management of the respective national company of Deutsche Telekom group. The contact shall be available for technical/non-technical aspects.

Motivation: In the event of a security incident, it must be possible to deal with the matter quickly and competently. In order to prevent avoidable delays, a contact person is essential.

ID: 3.08-1/2.7

Req 2	The hosting provider / SaaS provider must provide a telephone line with 7x24 availability to accept all security matters. The hosting provider / SaaS provider must ensure the availability during regular business hours, if not stated otherwise in the SLA.

Motivation: In the event of a security incident, it must be possible to deal with the matter immediately. Availability at all times is therefore essential.

ID: 3.08-2/2.7

Req 3	The hosting provider / SaaS provider must have an annually updated security framework, implement it and submit it to the purchaser or a person nominated by the purchaser on request.

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

ID: 3.08-3/2.7

Req 4	The hosting provider/SaaS provider must establish processes and process documentation to respond quickly and efficiently to vulnerabilities and security incidents and to present them to the purchaser or a person nominated by the purchaser on request.

Motivation: In the event of a security incident, it must be possible to deal with the matter quickly and competently. A process description including training on the processes is essential to prevent avoidable delays.

ID: 3.08-4/2.7

Req 5	The hosting provider / SaaS provider must ensure that the purchaser and possibly also the Security Management responsible must be informed without delay of a security incident / security vulnerability with relevance for Deutsche Telekom Group systems / data.

Motivation: In the event of a security incident, the Deutsche Telekom Group must be able to react timely, e.g. to perform mitigating actions, inform Deutsche Telekom customers and press.

ID: 3.08-5/2.7

Req 6	The hosting provider/SaaS provider must technically ensure that data of the purchaser based on his request or the request of the security management will be made unavailable within one hour.

In case of dedicated hosted systems, a complete shutdown / separation from the network is a suitable solution for this requirement. Who may be the requestor of such a measure shall be determined for each system individually.

Motivation: In the event of a security incident, it must be possible to quickly isolate corrupted systems for forensics and to avoid further damage.

ID: 3.08-6/2.7

Req 7	The hosting provider / SaaS provider must grant Deutsche Telekom group internal security units appointed by the customer the right to perform its own audits of the hosting infrastructure used by it (supplier audits).

The hosting provider shall support the customer and the Deutsche Telekom Group units named by it with the implementation. In detail, support means that

- test accounts are made available
- relevant security documentation / information is visible
- accesses (technical/physical) are made available.

Motivation: The principle of double checking shall be ensured by assigning different auditors.

ID: 3.08-7/2.7

Req 8	The hosting provider / SaaS provider must perform a security review of its hosting environment every 12 months and provide the results to the customer and the Deutsche Telekom Group units named by it on request.

The scope of the audit should include at least the network infrastructure and the basic applications such as Apache or Oracle.
Apart from checks on the basis of port scanners and version scanners (communication shall be checked for anomalies.

Motivation: In the event of an undiscovered security incident, it can be detected by means of a review. Furthermore, cyclic checking of the systems enables adjustment to new developments and problem areas that have not been recognized up to now.

ID: 3.08-8/2.7

Req 9	To ensure the sustainability of the security review/audit measures, subsequent to the audit the hosting provider/SaaS provider must submit a appropriate time schedule for the near future elimination of the vulnerabilities to the purchaser or a person nominated by the purchaser on request.

At least network infrastructure and basis applications such as Apache or Oracle must be in scope of the Audit. Besides portscans also analysis of logfile anomalies and network traffic anomylies should take place.

Motivation: Tracking of events is possible on the basis of an action plan including time lines. This ensures that temporarily tolerated system states are resolved within agreed times.

ID: 3.08-9/2.7

Req 10	The hosting provider/SaaS provider must ensure that internal information made available by the Deutsche Telekom Group or at its request is only accessible (subject to the “need-to-know” principle) to a small group of persons who are essential for executing the order.

Motivation: Narrowing down data to the smallest possible group of addressees minimizes the risk of data being

passed on.

ID: 3.08-10/2.7

Req 11	Within the context of the hosted Deutsche Telekom Group applications, the hosting provider/SaaS provider must always be able to provide up-to-date meaningful information about hardware, the operating system, software, the architecture, contacts, hardening and escalation possibilities to the customer, free of charge.

Motivation: A high level of security can be ensured only if all participants in the process work in compliance with the same standards and these are known.

ID: 3.08-11/2.7

Req 12	The hosting provider/SaaS Provider must ensure that redundant systems are accommodated in separate fire sections at the request of the Deutsche Telekom Group.

Motivation: Operating redundant systems in separate fire sections offers protection against physical damage such as e.g. water and fire.

ID: 3.08-12/2.7

Req 13	The hosting provider/SaaS provider must ensure that additional security measures such as lockable computer cabinets for secure hosting operation are provided for applications (systems) designated beforehand by the Deutsche Telekom Group as relevant.

Motivation: Breaking down the security zones makes it possible to establish a higher security level for systems requiring special protection without all systems having to be protected generally at high cost.

ID: 3.08-13/2.7

Req 14	The hosting provider/SaaS provider must ensure that customer applications / data are operated in a logically and, if possible, even physically separate location from other customers' applications/ data (if the type of application allows physical separation at all).

The minimum information that should be stored is which individual/ID accessed a building when. Storage can take place, for example, in the form of a separate database solution.

Motivation: Separation of systems according to customer minimizes the risk of systems influencing one another and the risk of a lower security level of a system of one customer of the hosting provider jeopardizing a Deutsche Telekom Group system.

ID: 3.08-14/2.7

Req 15	The hosting provider/SaaS provider must ensure that MZ systems are not directly accessible from the Internet.

MZ stands for "militarized zone", i.e., the zone containing business-critical back-end systems, which may only be addressed by external sources via the detour of systems in the "demilitarized zone" (DMZ).

Motivation: Termination of all traffic in the DMZ enables more in-depth protection of all MZ systems.

ID: 3.08-15/2.7

Req 16	The hosting provider/SaaS provider must ensure that the actual data management of an application always takes place in zones not reachable from the internet.

Motivation: Placing the data management systems in the MZ minimizes the direct risk of attack.

ID: 3.08-16/2.7

Req 17	The solution architecture must be in accordance with industry best practices including separation from functional blocks.

Besides the architecture itself the building components such as database and web server must not be hosted on the same logical system.

Motivation: By using industry proven approaches, the costs for implementing security, reliability and availability can be reduced and the attack vectors can be limited.

ID: 3.08-17/2.7

Req 18	The hosting provider/SaaS provider must provide measures/tools for detecting attacks and use them.

Suitable measures at this point can be:

- Log file analysis tools (e.g., access/error logs), not meaning simple texteditors
- Firewall systems
- Intrusion detection systems
- Network monitors

Intrusion prevention systems are not mandatory from the current technology perspective.

Motivation: Damage can be averted be detecting attacks early.

ID: 3.08-18/2.7

Req 19	The hosting provider/SaaS provider must provide, implement and document suitable measures and processes for warding off attacks from the Internet on the systems/platforms.

Suitable measures at this point can be:

- Routers with traffic shaping
- Firewall mechanisms
- Multiple peering points

Motivation: Only with a timely response and proactive protection measures, a suitable availability of instrastructure can be guaranteed.

Implementation example: One example of suitable segmentation is the use of a separate VLAN.

ID: 3.08-19/2.7

Req 20	The hosting provider/SaaS provider must ensure the creation of a DMZ/MZ by using suitable active network elements (at least packet filters).

A demilitarized zone (DMZ) designates a computer network with security-controlled possibilities of access to the server connected to it. Only DMZ systems may be accessed from the external network/Internet.

Motivation: Establishing DMZ/MZ zones without using active network elements does not offer any additional protection.

ID: 3.08-20/2.7

Req 21	The hosting provider/SaaS provider must ensure that administrative access to hosting systems containing Deutsche Telekom Group applications/data can take place only via approved and reliable encrypted protocols/entry points such as SSH.

Motivation: The risk of eavesdropping on administrative identifiers is clearly reduced by the use of encrypted protocols.

ID: 3.08-21/2.7

Req 22	The administrative access to Deutsche Telekom group systems from the internet must be realized via dedicated admin networks or hopping servers (VPN based).

Motivation: The risk of eavesdropping on administrative identifiers is clearly reduced by the use of encrypted protocols.

ID: 3.08-22/2.7

Req 23	Depending on the information being worked with in the hosted service, the hosting provider/SaaS provider must ensure that its employees are obligated to comply with country specific telecommunications privacy and data protection laws of the respective legal entity.

In case of hosting personal data according tot he national privacy law, this requirement must be fulfilled by a commissioned data processing agreement.

Motivation: To ensure that the data forwarded or accessible to the hosting provider is protected, the employees must be made aware in a suitable manner that the data requires protection and they must be obligated to observe this data protection requirement (where legally required).
For customer details in Germany this means, for example, the conclusion of a contract for commissioned data processing and the obligation of the employees to comply with telecommunications privacy and the German Federal Data Protection Act (Bundesdatenschutzgesetz).

ID: 3.08-23/2.7

Req 24	The hosting provider/SaaS provider must ensure that only authorized administrators/processes may set up, modify, delete, activate, block and view users subject to the “need-to-know” principle.

Motivation: Narrowing down certain critical functions to individual employees reduces the general risk of misuse.

ID: 3.08-24/2.7

Req 25	The hosting provider/SaaS provider must ensure that an administrator or user is never allowed to issue more rights/permissions than are granted to him.

Motivation: Narrowing down certain critical functions to individual employees reduces the general risk of misuse.

ID: 3.08-25/2.7

Req 26	The hosting provider/SaaS provider must ensure that systems operated for the Deutsche Telekom Group are kept free from harmful software e.g. by the use of up-to-date virus scanners or other technical options.

In the context of web applications with upload functions this refers to automatic scanning of uploaded data by the system.

Motivation: Harmful software represents a considerable risk for operation because access through such software to other systems cannot be ruled out, for example.

ID: 3.08-26/2.7

Req 27	By means of regular checks (i.e., at least once a month), the hosting provider/SaaS provider must ensure that only absolutely necessary software is installed/activated on the systems operated for the Deutsche Telekom Group. The definition for the needed software usually is delivered from the SaaS/hosting partner.

This requirement must be considered in the context of the commissioned service. This means that this requirement does not apply to managed services where the service provider is responsible for the service.

Motivation: Regular checks can contribute towards ensuring that the security level stays at a known level and unnecessary software can be ruled out as an additional source of danger.

ID: 3.08-27/2.7

Req 28	By means of regular checks (i.e., at least once a month), the hosting provider/SaaS provider must ensure that only necessary services defined by the hosting/SaaS partner run on the systems operated for the Deutsche Telekom Group.

This requirement is highly context sensitive, e.g. it is not valid for managed services as the service offerer hereby is responsible for the service.

Motivation: Regular checking can contribute towards ensuring that services needed for administrative or support purposes are ruled out as an unnecessary source of danger.

ID: 3.08-28/2.7

Req 29	The hosting provider/SaaS provider must ensure that systems/applications/middleware operated on behalf or at the request of the Deutsche Telekom Group are hardened based on “best practice” approaches.

This requirement depends on the scope of the actual hosting agreement and shall be implemented on the basis of a complete hosting above and beyond a housing model.
A good set of best practices can be found in the www.csisecurity.org webpage.

Motivation: Each hardened system boosts safeguarding of the entire data center.

ID: 3.08-29/2.7

Req 30	The hosting provider/SaaS provider must verifiable ensure a documented, implemented process for patch management.

Motivation: Current patchtstatus reduces the risk of intrusions.

ID: 3.08-30/2.7

Req 31	The hosting provider/SaaS provider must verifiable ensure that applications/operating systems always have an up-to-date patch level, which enables a flawless operation.

Motivation: Systems constantly kept at an up-to-date patch level are less vulnerable to attack from external/internal hackers. An up-to-date patch level therefore represents an elementary component of a secure system.

ID: 3.08-31/2.7

Req 32	The hosting provider/SaaS provider must establish, actively practice and test a backup and recovery process and present it to the Deutsche Telekom Group on request.

Motivation: In the event of damage, backups and recovery processes enable live operation to be resumed quickly and therefore contribute towards quality of operation.

ID: 3.08-32/2.7

Req 33	The hosting provider/SaaS provider must ensure that only actively supported software is utilized by the supplier/manufacturer/developer.

Motivation: If an error should occur in a software component, a guarantee that patches can be provided within a short period of time is only possible if the software list is actively maintained.

ID: 3.08-33/2.7

Req 34	All input to the application must be validated in accordance with industry best practices.

Motivation: By using industry proven approaches, the costs for implementing security, reliability and availability can be reduced and the attack vectors can be limited.

ID: 3.08-34/2.7

Req 35	Secure configuration of database systems must be according to industry best practise.

Hardening covers e.g. the following aspects

- having multiple database instances on the same system requires the operators to also be the same
- unused / unnecessary packages and functions must be deleted
- Default passwords, roles and accounts must be deleted
- databases must be operated following the least privilege and need to know principles

Motivation: By using industry proven approaches, the costs for implementing security, reliability and availability can be reduced and the attack vectors can be limited.

Implementation example: Please refer to Deutsche Telekom Group Security Requirements on Databases for an example. Additional good resources are e.g. CIS (http://www.cisecurity.org) or the homepages of the producers.

ID: 3.08-35/2.7

Req 36	The hosting provider/SaaS provider must ensure that access to internal systems and applications of the provider is logged.

Logging should at least cover the last seven days and should include access to account management/system administration systems.

Motivation: Logging the access to internal systems enables effective clarification of all manner of incidents.

ID: 3.08-36/2.7

Req 37	The hosting provider/SaaS provider must ensure that only personalized accounts are used to perform internal work.

Internal work within the scope of this requirement includes:

- Setting up new accounts
- Extending firewall rules
- Any form of network administration measures

Motivation: In the event of damage, the use of group accounts does not permit neat investigation.

ID: 3.08-37/2.7

Req 38	The hosting provider must ensure a documented, implemented process for account management.

Motivation: Only by means of an established process is it possible to ensure that both newly hired individuals and individuals leaving the company are not provided with unauthorized access.

ID: 3.08-38/2.7

Req 39	Access control and authentication mechanisms must be in accordance with industry best practices.

Motivation: By using industry proven approaches, the costs for implementing security, reliability and availability can be reduced and the attack vectors can be limited.

ID: 3.08-39/2.7

Req 40	The hosting provider/SaaS provider must ensure that confidential information such as access data is stored and transmitted only in an encrypted form based on current encryption standards.

Encryption of access and usage data on the hard disk should correspond to a strength of AES 256 bits.
For transmitting TLS >=1.2 with PFS cipher suites must be used.

Motivation: Coding of the data stored on data carriers makes it difficult for hackers to gain access to critical data .

ID: 3.08-40/2.7

Req 41	The hosting provider/SaaS provider must back up/protect data in such a way (technically, physically and organizationally) that unauthorized parties cannot gain access to the data.

Motivation: As backups may contain confidential information and generally enable conclusions to be drawn as to defensive measures, safeguarding of backups (by locking them away in a steel cabinet) is imperative to back up the information of the Deutsche Telekom Group without any gaps.

ID: 3.08-41/2.7

Req 42	The hosting provider/SaaS provider must provide a process for secure destruction of data carriers / secure deletion of data, have put this process into practice and be able to produce evidence of the destruction of data carriers.

Motivation: Without secure deletion of data carriers, there is an immanent risk of data loss which must be explicitly kept to a minimum.

ID: 3.08-42/2.7

Req 43	All data handeled by the application must be confidentiality and integrity protected in accordance with industry best practises.

Motivation: By using industry proven approaches, the costs for implementing security, reliability and availability can be reduced and the attack vectors can be limited.

Implementation example: Please refer to Deutsche Telekom Group Security Requirements on Application Development as an example.

ID: 3.08-43/2.7

Req 44	The hosting provider/SaaS provider must ensure, that only defined log files, which only contain data regarding accounts and/or the service usage by end customers n the role as DTAG business partner, partner or employee of Deutche Telekom group, will be securely transmitted to Deutsche Telekom group on request within 24 hours.

The basic assumption here is that clarification within the scope of the data privacy laws has taken place internally at the Deutsche Telekom Group in advance and that only operational implementation takes place at the external partner. Data can be transferred on the basis of encrypted e-mail communication, for example.

Motivation: In the event of an operational disruption, it must be possible to respond at short notice to maintain operation.

ID: 3.08-44/2.7

Req 45	The hosting provider/SaaS provider must protect log files against loss and not approved access in an adequate and tamper-proof manner.

Motivation: As log files generally allow conclusions to be drawn as to defensive measures, safeguarding of log files is imperative to avoid pointing out additional attack vectors to hackers.

ID: 3.08-45/2.7

Req 46	Fraud prevention must be implemented as appropriate based on industry best practices.

Motivation: By using industry proven approaches, the costs for implementing security, reliability and availability can be

reduced and the attack vectors can be limited.

ID: 3.08-46/2.7

Req 47	The virtualisationsoftware must be operated in compliance with the hardening guidelines / best practices of the vendors.

ID: 3.08-47/2.7

Req 48	The communication channel between virtual machine and virtualisation server must be closes / secured as possible.

ID: 3.08-48/2.7

2.1. Legal aspects

Req 49	In case of subcontracting the hosting provider/SaaS provider, if he receives access to confidential data from Deutsche Telekopm group (including personal related data), must ask for permission to use dedicated subcontractors.

Motivation: A high level of security can be ensured only if all participants in the process work in compliance with the same standards and this is documented by means of a contract.

ID: 3.08-49/2.7

Req 50	The hosting provider/SaaS provider must sign a Deutsche Telekom group Non Disclosure Agreement (NDA) with the customer, if the provider can gain business related internal information from the Deutsche Telekom Group.

An NDA SHALL be concluded between the customer and the hosting provider to ensure that any information that has been passed on or made accessible remains confidential.

Motivation: By signing an NDA, information of the Group requiring protection can be forwarded on the basis of the "need-to-know" principle.

ID: 3.08-50/2.7