Security requirement

Operations

Deutsche Telekom Group

Version	2.1
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
	3.61	Security requirement

Version	State	Status
2.1	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
Requirements for secure system operations.

Table of Contents

1. Introduction

This 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 security requirement defines the key operational and procedural/organizational security requirements for the production phase of a system. It is directed, in particular, at the organizations commissioned with operating systems. It may be used when preparing agreements between the business unit (as customer) and the operator (as the contractor) and complements the agreements on information security concluded with hardware/software suppliers.

The following topics are not or not fully covered by this document:

- System layout (see technical security requirements)
- Physical security
- Human resources security
- Business continuity management
- Emergency management
- Fraud detection
- Requirements regarding the protection of classified information
- Data protection topics, e.g., conclusion of an Data Processing Agreement (DPA)
- Office communications

2. Organizational matters

2.1. System responsibility

Req 1	For every system there must be a system owner who is to assume responsibility during the operating phase.

The system owner for operations (technical system owner) clarifies the respective system rolls and task allocation with the system owner of the commissioning business unit (functional system owner). Together they share the collective responsibility of implementing the defined roles and in particular the operational tasks for:

- Implementing, and maintaining the data protection and security concept (SDSK)
- Cyclically reviewing compliance with the regulations for data privacy and information security
- The security status of all installed software (in particular patch management)
- Timely availability of security updates by the supplier/manufacturer
- Compliance to the safety requirements for established communication links
- The up-to-dateness and completeness of information (system and machine lists) stored in an inventory
- The existence of a security and data privacy approval upon handover to the operation
- Testing and maintaining of existing emergency plans
- Committing and training users and service providers to comply with security regulations
- Appointing a contact who is able to accept and process security-related inquiries at the agreed times
- Ensuring proper decommissioning or migration of the system. This includes optionally the archiving and / or deletion of data, the withdrawal of access and network releases and updating of inventory data

The (technical) system owner is appointed by name and documented in an appropriate place, typically in the system inventory of the responsible business unit. This also applies to services that are obtained from a cloud.

Motivation: If no system owner has been clearly appointed, there is a risk that security-critical measures are not taken and implemented in time or even not at all.

ID: 3.61-1/2.1

2.2. Contact

Req 2	There must be a contact option in place via which security-related inquiries are accepted at agreed times and processed as declared.

Inquiries regarding the security status (e.g., in the case of an security incident) and security adjustment requests (e.g., installing patches) must be processed in a timely manner as regulated before. For this, a general contact must have been defined who can accept such inquiries and requests at the agreed (support) times and forward them accordingly. This is usually a service desk that is ideally available 24/7.

The respective (technical) system owner must ensure that this contact has been appointed and is able to sufficiently process security-related inquiries.

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

ID: 3.61-2/2.1

3. Processes

3.1. Change Management

Req 3	Changes to systems must be subjected to a change process that has been defined in advance.

No changes shall be allowed to override the data privacy and security controls for a system or reduce their effectiveness. Such changes therefore have to be agreed taking into account the associated risk. The changes must be adequately authorized and appropriately documented.

It is recommended to test changes in advance and prepare rollback procedures. System documentation must be adjusted with regard to the changes.

In addition to a documented change management process, we recommend the implementation of additional typical operating processes that are closely linked to change management and together provide for secure operation:

- Configuration management – overview of the system/IT landscape
- Release management – controlled provision of new releases and (generally) new systems
- Incident management – incident processing
- Problem management – elimination of the root cause of incidents
- Capacity management – provision of appropriate resources

If frozen zones are specified, it must be defined whether necessary security updates are imported during this time and, if so, how this is done. It must be specified how "emergency changes" are approved (possibly in advance depending on the type).

Motivation: Unauthorized changes pose a high security risk, this applies in particular if security relevant aspects of the change are not considered before.

ID: 3.61-3/2.1

3.2. Inventory and configuration management

Req 4	All components (machines, servers, network elements, etc.) must be known, added to the inventory, and mapped to a system so that clear responsibility is defined for every component. The mapping must be up-to-date.

The term "components" refers to all security-related elements here (these are usually active system components such as servers, firewalls, routers, etc. and are also referred to as "machines"). Shared elements like storage systems belongs to them also. All these components must be mapped to systems. Systems, in turn, are mapped to system owners so that clear responsibility for every component is ensured via this relationship. Before start of operation, it must be specified which parts and which information about each part must be included in such an inventory as a minimum for the purpose of a security-related assessment. Asset and configuration management are also part of an ITIL (IT Infrastructure Library) process framework that is used in many areas to manage IT systems.

Every system as well as every component/machine must also have a unique identifier via which the component/machine can be clearly identified.

Motivation: Without any system mapping and thus a system owner, swift action in the event of a security incident cannot be ensured.

Implementation example: With regard to implementation, we recommend a database (configuration management database, CMDB) that contains all components, systems, and their interrelationships. This CMDB then constitutes the system inventory and the machine lists. The necessary granularity and topicality can be defined on the basis of business relevance and the system status such as test/production.

With TASTE-OS (Telekom Automated Security Testing Engine – Offline Scanner, https://tos.telekom.de/), Telekom Security provides a tool for inventorying, collecting and evaluating security-relevant system configurations and the

patch status of machines.

ID: 3.61-4/2.1

Req 5	Current configuration data must be available for every system and all system components so that it is possible to perform a security-related assessment of the entire system landscape on the basis of this data at any time.

It is recommended to use a configuration management database (CMDB), which represents the source of all (security-) related information. This database may be set up centrally or locally (e.g., by organization or technologies used). The data documented in the CMDB is collected automatically where possible so that the up-to-dateness and accuracy of the data is ensured. Only a small amount of metadata or master data should be maintained manually or is provided by other systems. Manufacturer-specific as well as independent tools can be used for the automated documentation.

A CMDB may contain the system list, the system owners, and machine lists, or references to other tools that contain this data. As a data source, a CMDB should contain the necessary information on systems and machines for almost all operating processes. As a central component in the ITIL (IT Infrastructure Library) process framework, a CMDB is indispensable.

If detectable, the following information must be stored:

1. All machines and systems with an unique ID
2. Installed operating system, software and patch level
3. IP addresses (with identification of internal and/or external accessibility)
4. Communication relationships that have been set up
5. Association of every machine to a system and thus to a manager
6. Hostnames, DNS names (internal and external), and reachable URLs
7. Required licenses
8. Protection requirements of data processed on the system
9. Machine types (physical, virtual, container, serverless, ...)
10. (TLS-)Certificates used, their parameters and the names for which they were issued
11. Supplier and developer of the system and software, including maintenance information
12. 7x24 contact for (security) incident management and response
13. Criticality factor of the system and the risk category of the machines

The status of the data in the CMDB must be checked against the actual status on the machines and systems at regular intervals.

Motivation: Knowledge of the current system status is a requirement for a) checking whether a system is affected by a vulnerability or a security incident, b) to find machines and/or components in the presence of a vulnerability and c) recovery.

Implementation example: With TASTE-OS (Telekom Automated Security Testing Engine – Offline Scanner, https://tos.telekom.de/), Telekom Security provides a tool for inventorying, collecting and evaluating security-relevant system configurations and the patch status of machines.

ID: 3.61-5/2.1

3.3. Account management

Req 6	Access rights must be up to date.

A functioning identity and access management is required. That means specifically:

- There must not be any unauthorized physical/system access.
- Only necessary permissions (i.e., authorized in keeping with the system) may be granted.

- If access permissions are no longer required, they must be withdrawn timely in accordance with deadlines defined in advance.
- A centralized identity and account management system should be used which is connected (for permission of internal employees) to an appropriate HR system. Entrances and exits of employees is thus automatically detected and processed. For external persons a reliable data source must exist, or an internal employee is defined as a sponsor and is responsible for the permissions granted in terms of scope and duration.
- There should be a role-based access module may be used which combines individual rights under the tasks to be performed a group of people in a role.
- A role-based access model should be used, which combines individual permissions under the tasks to be performed in one role. Ideally, roles are always be filled twice (for deputies).
- Authorizations must be assigned by the 4-eyes principle.
- The system must support two-factor authentication when granting access with extensive rights (administrator).
- The status of the access permissions on the system (current situation) must be checked against the documented, authorized status (target situation) at regular intervals (at least once a year). The accounts themselves must be submitted to the functional business unit for consideration of the current demand.
- For systems that are not connected to a central identity and access management system, an authorization check must be carried out every 3 months at the latest.
- Compliance with the authorization concept must be checked by way of random samples.

Accesses and authorizations of machine-to-machine (M2M) connections must be managed just as carefully.

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

Implementation example: Use of a central IAM system, see YAM United - PSA - IAM https://yam-united.telekom.com/pages/psa/apps/wiki/wiki/list/view/bfb5c088-8205-4fdd-99ba-4133abfd376f.

ID: 3.61-6/2.1

3.4. Security incidents

Req 7	The handling of security incidents that put the confidentiality, availability, or integrity of a system at risk must be organized.

A security incident is an event that impairs the confidentiality, availability, or integrity of a system or the data contained therein in such a way that the company may suffer or has already incurred damage. A process must have been defined indicating how such incidents can be identified and classified, who must be notified in which time, who must be consulted in the event of escalation, and which options as countermeasures are defined. The content of such emergency plans must be known to all individuals involved in operations. If necessary, trainings for admins and system owners must be carried out for this purpose.

Options for the identification of security incidents (not exhaustive):

- Irregularities that are reported by a security information and event management (SIEM)
- Reports by an intrusion detection system (IDS), e.g., hacker attack, (d)DoS attack
- Log file analysis
- Compromised cryptographic keys
- Monitoring systems (technical incident)
- Report by employees or external staff

Example reporting channels:

- Officer on duty
- National Cyber Emergency Response Team (CERT) or company wide: cert@telekom.de, telephone +49 800

DTAG CERT
- National Situation Center or Group Situation Center
- (Functional) System owner
- Where agreed: (internal) customers

Possible countermeasures:
- The Arbor Peakflow platform can be used to avert a volume based Denial-of-Service attack (provided the system is connected to the DTAG IP2 network [AS3320]).
- System shut-down, depending on what was agreed with the funcional system owner – whether to protect the integrity of the data and taking shutting down the system (so that it is no longer available to the customer) or whether to ensure availability for the customer with the risk of data being copied, changed, or deleted.
- Setting of filters in firewalls or other upstream systems.

Motivation: Security incidents must be dealt with quickly and competently in order to avert potential damage to the company, employees and customers.

ID: 3.61-7/2.1

3.5. Vulnerabilities

Req 8	Information on vulnerabilities must be assessed. Depending on the resulting threats, appropriate countermeasures must be implemented if needed.

Vulnerabilities represent threats to systems if they can be exploited. This is why vulnerabilities that have become known must be assessed immediately to establish whether they pose a threat. Measures to avert or contain damage therefore have to be taken.

Possible procedure:
- Subscription to advisories from the suppliers and/or DTAG CERT (seehttps://dcert.de/)
- Use of the Security Operations Center (SOC), which uses monitoring to detect vulnerabilities and security incidents
- Identifying threats based on the criticality of the vulnerability, the potential scale of impact, and the protection requirement of the systems concerned
- Taking appropriate countermeasures per related system such as deactivating affected features, installing patches, restricting access by network based filters (firewalls), or shutting down the service

Motivation: Vulnerabilities that have become public knowledge must be examined and assessed immediately as regards the potential threat they pose. Countermeasures that are deemed necessary must be planned accordingly in order to keep the company free from damage.

ID: 3.61-8/2.1

Req 9	It must be ensured that systems receive all necessary security updates in accordance with the defined DT patch policy.

The DT patch policy specifies resolution times depending on the exposure level of the systems and the criticality of vulnerabilities (based on CVSS scores).

Maintenance windows have to be planned on a regular basis, which also take "Patch days" of manufacturers (such as Oracle, Microsoft, and IBM) into account.

It is recommended to use own repository servers that provide the manufacturers' software packages locally and are

able to check these software packages with regard to integrity (e.g. by the signature of the maintainer) before they are installed on systems.

After an update, checks must be carried out to ensure that all security settings are still enabled and no higher privilege levels have been granted to users or processes.

Motivation: Systems with an up-to-date patch status are less vulnerable to attack. An up-to-date patch level is therefore an elementary component of a secure system.

Implementation example: Patch Policy of Deutsche Telekom, see Policy Database.

ID: 3.61-9/2.1

3.6. Monitoring of security settings

Req 10	Security related settings of the system configuration must be checked against the agreed target status at regular intervals.

The system configuration must be checked for changes and compliance with the provisions (target status) with regard to security settings. Several parts have to be taken into account here: the integrity of firmware/hypervisor software/the operating system must be ensured through regular system configuration checks, ideally before boot-up. The possible communication relationships (e.g., firewall activations) must be checked against unauthorized changes. The security configuration of applications must be checked.

There must be rules in place as to how to deal with variances that are identified. If there is a suspected security incident, the relevant units/people must be notified immediately.

Motivation: Regular checks help to identify and stop faulty configurations and associated security leaks in good time.

Implementation example: A collector is set up to collect all relevant data on all systems and the information gained in this way is checked against provisions and standards. If such an automated process is not available, random samples must be audited manually.

With TASTE-OS (Telekom Automated Security Testing Engine – Offline Scanner, https://tos.telekom.de/), Telekom Security provides a tool for inventorying, collecting and evaluating security-relevant system configurations and the patch status of machines.

ID: 3.61-10/2.1

3.7. Security tests

Req 11	Vulnerability tests must be conducted at regular intervals for all systems depending on criticality and the threat situation at least at the "customer interface".

A distinction must be made between simple tests (automatic scanners) with which all accessible systems are subjected to a basic check on the "customer interface" as a minimum, and system-specific tests for which specific test cases were defined in advance. These are usually more in-depth tests for which it has been specified when and how often they can be performed without posing a risk to operations. The principles of "ethical hacking" are to be considered in this kind of penetration testing. The aim is to find vulnerabilities before others do.

Typically, the information about systems, interfaces and applications to be tested is stored in the configuration database (CMDB).

If such reference/test systems are available, new releases should be security checked before commencing production.

Motivation: Many security gaps can only be detected through regular testing (externally/on the customer side). Sometimes minor configuration changes to a piece of application software are sufficient to generate a security gap for the system. Tests are essential for finding these gaps before an attacker does.

Implementation example: With DTSP (Deutsche Telekom Scan Platform, https://dtsp.telekom-dienste.de/), Telekom Security provides a tool for a wide range of security tests.

ID: 3.61-11/2.1

3.8. Disaster management

Req 12	If emergency/disaster recovery measures were agreed, they must be checked, tested, and updated in accordance with the agreements.

Disaster recovery (DR) strategies must be tested for effectiveness at regular intervals. This includes simulation games, desk tests, and exercises. The results must be documented and used to improve the processes. A (functional) system owner with DR requirements must always be informed about the status of the DR capability of his operator.

Motivation: Without sufficient testing of emergency plans, the knowledge and routing in the event of an emergency is insufficient for implementing the plan efficiently and effectively.

ID: 3.61-12/2.1

3.9. Third-party maintenance and support

Req 13	Appropriate agreements must be concluded with suppliers and supporters in order to be able to respond to vulnerabilities, security incidents, and system failures that have become known.

In the event of security incidents, it may be necessary to cooperate with the supplier in order to ensure minimum processing times. Agreements on the timely provision of security fixes for the software, the replacement of defective hardware and, if required, special rules for disaster handling must be agreed with the supplier.

With regard to support cases, it must be specified how data, information, data media, or devices can be securely sent to the support partner or how internal systems can be accessed while complying with the applicable security requirements. The contact and the agreed support times must be known and should be stored in the CMDB where available.

Motivation: To be able to update or recover a system in the specified time, appropriate delivery agreements must be concluded with the suppliers.

Implementation example: The "Information Security Annex" will be agreed with the supplier as a component of the contract (handled via Procurement, see here in YAM United).

Use of the Vulnerability Advisory Service (VAS) from Telekom CERT, https://dcert.de/

ID: 3.61-13/2.1

Req 14	Third-party access for operating activities and support purposes (incident clearance, maintenance) must be controlled.

If third-party access from external networks is required, an access platform that has been approved for such usage must be used. It has to be ensured that access via this platform takes place in a controlled manner only. Depending on the indivual case and agreement, the following may be necessary:

- Activation following approval by an internal employee only
- Activation for a specific period of time only
- Revocation of the activation
- Target restriction: only requested systems are accessible
- Activity logging (Command Line / Graphical Interface)
- Session timeout control

- Deactivation on request
- Monitoring of authentication

Motivation: Ensuring control options for system changes performed by third-parties.

Implementation example: Use of the Telekom Technik Deutschland "CRD-Portal", see here in YAM United.

ID: 3.61-14/2.1

3.10. IDs, keys, and certificates

Req 15	Cryptographic keys and certificates must be renewed before the specified end of validity.

Certificates must be monitored so that they are replaced in accordance with a process defined in advance before they expire (if they are still required). We recommend being able to view the validity information of certificates in a data store to be able to issue and distribute new ones in time. An online check must be conducted as well to be able to check the actual installation status and compare it with the target status.

Depending on the intended purpose, very different validity periods are a sensible option for cryptographic materials.

Cryptographic material with need of protection, e.g., symmetrical keys (pre-shared keys), must always be transported via a secure channel.

Tip: Certificates should not be issued on February 29 as this expiry date might cause problems.

Motivation: Compromised key material can result in loss of integrity, confidentiality, and authenticity. Expired certificates frequently lead to application incidents.

ID: 3.61-15/2.1

Req 16	Access data like passwords and cryptographic keys must be protected against misuse.

Passwords of personal accounts may never be shared.

For passwords of technically needed system accounts (eg root, Oracle-Admin) must be defined and documented

- who knows them
- how and how frequently they are replaced
- how it is ensured that they are changed when an authorized person leaves
- how it can be ensured that other individuals can get access in an emergency

If passwords or cryptographic keys are stored for emergency access, they must be safe from unauthorized access (in a safe, physically or electronically). It must be specified whether a new password/key has to be generated and set up after accessing this credential. If possible, passwords for accessing privileged accounts are stored in a PAM (Privileged Access Management) system.

Continuously used cryptographic material must be stored securely and protected against access from unauthorized individuals. For example, it is best to store personal SSH keys on smartcards and protect them with a PIN. In the case of SSH agent forwarding, an interaction should be switched on so that nobody can misuse the key remotely.

Private keys of TLS(SSL) certificates must be stored with minimum access rights and protected with a passphrase that is stored separately from the key. Transport should only take place in encrypted form if at all.

Motivation: To ensure that only authorized individuals can access systems.

ID: 3.61-16/2.1

Req 17	Secrets used for automation in development, deployment and operations of applications must be protected by a Secrets Manager.

A Secrets Manager can provide the interfacing process or application with the required authentication data exactly where needed during runtime. Secrets can be easily updated and their use is automatically registered in the audit logs of the Secrets Manager.

Motivation: Using a Secrets Manager reduces the exposure of secrets and prevents their leakage. Access logs provide transparency in case of a security incident.

Implementation example: Examples include HashiCorp Vault, AWS Secrets Manager, Azure Key Vault and Kubernetes Secrets.

ID: 3.61-17/2.1

Req 18	Potentially compromised passwords, keys, or certificates must be deactivated and replaced immediately.

If it is suspected that a password, cryptographic key oder certificate has ended up in the wrong hands, any access that can be gained with it must be revoked immediately. A change of the authentication data is mandatory under the following general conditions:

- when the change of initial passwords is not technically enforced
- when it is suspected that third parties have obtained knowledge of authentication data
- when authentication data had to be used in a presentation and thus became known to the participants
- following the completion of work (e.g., work performed by a suppliers on site) for which authentication data was communicated deliberately
- when someone must be provided with relevant data media (system disks, magnetic tapes), e.g., for the purpose of securing circumstantial evidence

Motivation: To prevent misuse of an access authorizatrion, the authentication data must be changed when knowing a compromise.

Implementation example: Telekom Security's "ID alarm" can also be used to detect compromised accounts, see https://digital-schutzpaket-id-alarm.telekom.de/.

ID: 3.61-18/2.1

4. System management and tools

4.1. Administrative workstation

Req 19	The security of workstations for (interactive) administration of production systems must be consistent with the protection needs of these systems.

Depending on the protection requirements of the systems to be administered, their criticality, size and general reasonableness, appropriate measures to secure the workstations must be taken to avoid compromising production systems in this way. Appropriate and proportionate measures have to be selected per system, customer or environment. Possibilities of securing workstations are:

- Use of special admin workstations completely without standard office capabilities, so called "Privileged Access Workstation" (PAW)
- Workstations do not make use of unprotected access to the Internet, the WWW and to E-Mail
- No direct access from Office workstations (standard office communication) to productive systems with the role of an administrator
- Use of jumphosts for regulating access (possibly a logging jumphost in case of special requirements and subject to corresponding agreements)
- Use of appropriate (graphical) terminal solutions
- Automatic access blocking: if a workstation or the terminal is inactive, a (password-) protected screensaver must be automatically activated using the mechanisms of the operation system (or manually activated prior to that)
- The workstation provides use of two-factor authentication on the target system
- File transfer from/to the system only via intermediate systems with malware scanners

Potentially insecure functions may not be used. Local port forwarding, tunnels, or gateway ports, for example, must not be activated in general when using an SSH client, but can be activated in a controlled manner in individual cases.

In order to avoid man-in-the-middle attacks, the identity of the target system must be checked: when logging in via SSH, the SSH host key must be checked, for example. This requires the host keys to be made available in a suitable manner. With Windows logins, the Remote Desktop Protocol (RDP) version 6.0 or higher can be secured with certificates or Network Level Authentication (NLA). Obsolete access protocols such as Telnet or FTP do not provide for any ways to reliably check the target system apart from the IP address as they do not offer cryptographic authentication.

Motivation: Any compromise caused by infiltrated malware (per email or from web) or by unauthorized users must be prevented.

ID: 3.61-19/2.1

4.2. System management and monitoring

Req 20	Additionally installed software for operation purposes (e.g., tools, monitoring and management agents) must be examined and approved by security.

If a system uses standardized system management/monitoring tools, a reference or "customer information" on the use of these tools must be noted in the system description. If individual solutions are implemented, they must be included in the system description.

It must be ensured that these tools can only be used to perform the activities intended for them. All tools required for operation generally need to be run with minimal privileges. If additional software is installed for operation purposes, the following aspects must be taken into account:

- Agents must not be run as network daemons that can be accessed remotely
- The initiation of agent communication depends on the trust relationship between the involved parties and the

data to be transmitted
- No write access for the user/processes of agent software that only performs monitoring functions
- Sufficient authentication of the agents against the management server and vice versa
- Use Tools only for the intended purpose. For example, a backup system, which was implemented purely for internal data / systems, may not be misused for backups from externally accessible machines.

The general rule is that less is more. Every additional tool offers more opportunities for attacks on the actual system.

Motivation: Additionally installed active management and monitoring software represents an additional threat to any system. For the security-related assessment of a system, all components installed must be known and may not be subsequently installed after commissioning without security approval. System management and monitoring software must not be misused for purposes for which it has not been planned and approved.

Implementation example: If sniffer tools such as tcpdump and wireshark are needed in operations, firstly they must not be installed permanently and secondly the graphic analysis may take place on another system (special designated workstation) so that the live system is only used to collect the data.

ID: 3.61-20/2.1

4.3. Installation and configuration

Req 21	The integrity and authenticity of software and configurations used must be ensured.

Upon the initial installation of a system, in subsequent installation processes, and when importing upgrades/updates (especially patches) it must be ensured that non-compromised original software and authorized configuration files are used. These may only be used from trusted sources.

Authentication mechanisms implemented by the manufacturer (digitally signed). must be used where available. Usually downloaded software (at least TLS authenticated and secured) can be checked against checksums provided on a different, secure channel.

Motivation: To ensure the integrity and authenticity of the software installed and the configuration used.

Implementation example: The use of proprietary, monitored repository servers and version management systems (e.g., GIT) like https://devops.telekom.de/.

ID: 3.61-21/2.1

4.4. Temporary files

Req 22	Data with need of protection that was temporarily set up by an administrator must be immediately deleted, encrypted, or otherwise protected against unauthorized viewing.

Temporary files may contain data requiring protection. Backup files of the system configuration or a network recording that is to be copied to another system for further processing, for example, contain data that must be protected against unauthorized viewing. If such data can not or should not be (safely) deleted immediately after their generation, all unauthorized access must be prevented.

Storing data on mobile data media is to be avoided due to the high risk of loss. However, if storing data on such media is unavoidable, the data stored thereon must be encrypted. Any data on this media that is no longer needed is to be immediately erased. The devices used must be protected against loss/theft where technically feasible.

Motivation: Protection against unauthorized viewing by third parties.

ID: 3.61-22/2.1

4.5. Security software

Req 23	Security software must be kept up to date at all times.

Security software includes, for example, anti-virus solutions (on workstations and servers, if used) as well as intrusion detection systems. To ensure that they detect as much malware and as many attacks as possible, they and their configurations, e.g. signatures, must be kept up to date. Checks must be carried out to establish whether these updates are carried out successfully.

Content filters on (web) proxies, spam filters on e-mail systems, both incoming and outgoing, and certificates (revocation lists) stored in a PKI must be kept up to date.

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

ID: 3.61-23/2.1

4.6. Logging

Req 24	Security related events must be forwarded to a central logging system and continuously monitored.

All systems are exposed to security threats, the identification and analysis of which is made possible centrally by a SIEM (Security Information and Event Management). For this purpose, all security-relevant logging data must be forwarded to a central system.

The log data originate from operating systems and applications. Furthermore, intrusion detection/prevention systems (IDS/IPS) can identify attacks by analyzing the network traffic that cannot be detected by a single system. An IPS can also be used as protection against denial-of-service attacks. If such an attack is detected, a corresponding system (Arbor Peakflow) can be activated in the IP2 backbone (please contact DTAG CERT), which offers opportunities to filter volume based attack traffic.

In the context of the automatic analysis of the forwarded logs, the main focus is on the threat situation of all systems connected to the SIEM and interactions in order to be able to initiate appropriate incident response processes and measures.

The time stamps of the logs must be correct – it is therefore essential to have a time synchronization of all systems supplying data. Logs shall be gathered in a common language, english is preferred.

Motivation: The task of the SIEM is to automatically analyze the incoming logs from the systems for security-relevant events and, in the event of detection by the incident response teams (CERT and SOC), to inform the relevant owners or persons responsible for the systems. Without (proactive) analysis attacks and attempted attacks can usually not or only after effects of damage be detected.

Implementation example: MSAS (Magenta Security Analytics System) is the central SIEM in DTAG, which can be reached from almost all networks and cloud platforms used. The following links list details that are necessary for connection and setup (incl. downloads of the available agents for Windows, Linux and Unix systems):

- MSAS-Syslog:https://yam-united.telekom.com/pages/cert/apps/content/msas-syslog
- MSAS in general:https://yam-united.telekom.com/pages/cert/apps/content/msas

ID: 3.61-24/2.1

4.7. Communication relationships

Req 25	The set of rules for all communication relationships must meet the current and documented requirements and be understandable.

A communication matrix documents the communication links between and within systems. Routing entries and firewall activations are performed on the basis of the communication matrix. Changes must be documented so that the communication matrix always reflects the current state.

Actual existing links must be compared with the documented target state at regular intervals. Activations that are no longer required must be removed from firewalls and other filtering (network) elements.

Motivation: Communication options that are no longer required and thus no longer permitted represent an unnecessary threat to the systems.

ID: 3.61-25/2.1

4.8. Restorability

Req 26	It must be possible to restore a system and its data in accordance with agreed parameters following any unplanned downtime.

Restore tests must be conducted in line with requirements and agreements. If a backup was chosen as the restore method (full/incremental), the frequency and depth of backups as well as the type of data backed up are dependent on the protection level required for the system, e.g., permanent mirroring of data on a different data medium at a different location (compare recovery point objective, RPO, and recovery time objective, RTO).

Backup data media should be stored at a suitable distance (minimum requirement: in a different fire zone). It must be checked whether the backup data needs to be encrypted and/or archived and how this can be done. Backup data may only be called up by authorized individuals and systems. It must be checked whether any confidential data is to be excluded from the backup (e.g., private keys of TLS certificates).

A traditional backup may be omitted if the system functionality can be restored in a different way. If there is no application data to be backed up, the system can be rebuilt purely on the basis of templates and information stored in a configuration database. This can go as far as re-installing entire system environments including all interfaces based on the configuration data stored.

Motivation: Backup and restore options make it possible to restart operation quickly in the event of damage.

ID: 3.61-26/2.1