

Requirements for

IT operating manuals

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Requirements for IT operating manuals | |  |
| Number | [Number] | |
| Issued on | 18.04.2024 | |
| Through | Chief Information Security Officer | |
| Entry into force | 01.07.2024 | |
| Scope of application | SÜDVERS Group | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last review | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Documented procedures must be established for operational activities related to information processing and communication facilities

The operating procedures must be documented and made available to all users who require them.

The operating procedures must include operating instructions, including (but not limited to):

* Description of ICT assets, including documentation of all of the following:
  + responsible employees
  + secure installation, maintenance, configuration and deinstallation of ICT systems;
  + Management of information assets used by ICT assets, including their automated and manual processing and handling;
  + Identification and control of obsolete ICT systems;
* Location of the system
* Information on the control and monitoring of ICT systems, including all of the following:
  + Requirements for the backup and recovery of ICT systems;
  + Planning requirements, taking into account the dependencies between the ICT systems;
  + Logs for audit trails and system log information;
  + requirements to ensure that the performance of internal audit and other tests minimizes disruption to business operations;
  + Requirements for the separation of ICT production environments from development, test and other non-production environments.
  + Requirements for carrying out development and testing in environments that are separate from the production environment;
  + Requirements for carrying out development and tests in production environments.
* Arrangements for access control (including the roles and responsibilities used);
* Monitoring procedures such as capacity, performance and safety;
* Planning requirements, including dependencies on other systems, earliest order start and latest order completion;
* System restart and recovery procedure in the event of a system failure;
* Maintenance instructions
* Contact for support and escalation including external contact for support in the event of unexpected operational or technical difficulties;
* Instructions for dealing with errors or other unusual conditions that may occur during order execution, including restrictions on the use of system utilities; including the following:
  + Procedures and protocols for dealing with errors;
  + Support and escalation contacts, including external support contacts in the event of unexpected operational or technical problems;
  + Procedure for restarting, rolling back and restoring the ICT system for use in the event of an ICT system malfunction
* Support and escalation contacts, including external support contacts in the event of unexpected operational or technical difficulties;
* special instructions for issuing and handling media, such as the use of special stationery or the management of confidential issues, including procedures for the secure disposal of issues from failed jobs
* Deviations from defined standard IT service management processes
  + Change management
  + Backup and restore
  + Malware protection
  + Time synchronization
  + Vulnerability and patch management
  + Event management (in particular the management of audit trail and system log information)
  + Management of security incidents
  + Capacity management (in particular monitoring procedures)