

Security Policy   
3rd party Service Provider Management management

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Security Policy 3rd Üarty Service provider management | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 04.07.2022 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| 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 | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Table of contents

[1 Principles 4](#_Toc153355805)

[2 Objectives 4](#_Toc153355806)

[3 Controls 4](#_Toc153355807)

# Principles

Information risks must be identified and managed at all stages of the relationship with external service providers (including companies in the supply chain).

# Objectives

Protection of critical and sensitive information during processing by external service providers (including organizations in the supply chain) or during transmission between SÜDVERS and external service providers.

# Controls

There must be a documented process for managing the information risks associated with external service providers (including organizations in the supply chain). The process must be integrated into SÜDVERS' procurement process and include the information security function throughout the procurement process and service provider management lifecycle and include the following:

* IT service providers must be recorded in a DORA-compliant register
* Identification and evaluation of critical and sensitive information that can be passed on to external service providers
* Definition of additional requirements for information security (e.g. the right to audit)
* Assessment of the ability of the bidding service providers (both existing and new external service providers) to meet SÜDVERS' security requirements for the protection of critical and sensitive information
* Assessment of the risks to the information that a bidder may pose if it is awarded the contract
* Supporting the procurement team in the pre-selection of providers, taking into account information security requirements
* Review of bids to understand the extent to which each vendor can meet SÜDVERS' information security requirements
* Selection of reputable, reliable and approved service providers
* Clarification and agreement of warranty conditions
* Supporting the procurement team in contract negotiations and incorporating SÜDVERS' security requirements into the contract with the selected external service provider
* Monitoring the information security performance (based on the agreed security arrangements) for the external service providers and intervening to manage the risks (identifying remedial actions where necessary)
* Establishing a method for the exit, termination, renewal and renegotiation of contracts with external service providers in compliance with the requirements of the Service Level Agreements (SLA)
* the provision of alternative arrangements in the event that one or more external service providers are no longer available.

All services proposed by the service providers that are requested by SÜDVERS must be evaluated in order to:

* determine whether SÜDVERS' standard terms and conditions need to be supplemented by additional information security terms and conditions tailored to address specific information risks
* determine the level of support required from the information security function throughout the procurement process.

The assessment of the proposed services must include the following:

* Identification and classification of information that may be passed on to external providers or to which they may not have access
* Information risk assessment to determine information security requirements
* determining SÜDVERS' internal, commercial, contractual, governmental, legal and regulatory obligations to protect information (such as those in customer contracts, laws such as the EU General Data Protection Regulation 2016/679 (GDPR) and data protection requirements).

Based on an assessment of the information risk and SÜDVERS' obligations, safeguards must be established to protect SÜDVERS' business information that is shared with external service providers. The safeguards must cover the external service provider's information risk management arrangements and include at least the following:

* Safety management (such as safety orientation, strategy and assurance, safety policy and organization)
* Risk management (e.g. risk assessment, risk treatment and risk reporting)
* Compliance (e.g. commercial, contractual, governmental, legal and regulatory requirements)
* Implementation of penetration tests (whitebox as well as blackbos tests) for all IT services relevant to SÜDVERS
* Regular awareness training for all employees of the service provider
* Access management (such as access control, access control mechanisms and federated identity and access management)
* Information management (e.g. classification and handling of information, data protection and document management)
* Infrastructure management (e.g. configuration of servers and network devices, firewalls, wireless access, data backup and change management)
* Security management in the supply chain (e.g. in relation to procurement, subcontracting, outsourcing and cloud computing)
* Threat and vulnerability management (e.g. cyber security resilience, system and software vulnerability management, security event logging/management and threat intelligence)
* Emergency management and crisis management
* Protection of mobile computers and electronic means of communication (such as e-mail, collaboration platforms and voice communication services)
* Protection of applications and management of system development (e.g. the life cycle of system development)
* physical and environmental security and business continuity (e.g. business continuity planning, arrangements and testing)
* Security monitoring and improvement (e.g. security audit, security and compliance monitoring and information risk reporting).

The Information Security Officer should assist the procurement team (e.g. by using an addendum to the information request) to obtain details of each supplier in relation to the following aspects:

* Ability to meet SÜDVERS' information security and regulatory compliance requirements
* Impact on the threats and vulnerabilities associated with SÜDVERS' information when stored and processed in the bidder's and its suppliers' systems (e.g. in the supply chain)
* Level of experience and maturity of the technology used to provide the required services
* Maturity level in managing information security and implementing security measures
* the geographical location and that of its suppliers and subcontractors
* existing security measures (including governance, risk management and compliance)
* Willingness to improve information security arrangements to meet SÜDVERS requirements and compliance obligations.

The body responsible for information security must verify the information provided by each provider (e.g. their response to the information request) in order to:

* determine the need for further investigation of a bidder's information security capability (e.g. due to insufficient information from a bidder)
* define the security requirements that must apply over and above the standard information security conditions of SÜDVERS
* Supporting the procurement team in the pre-selection of suppliers (e.g. drawing up a list of selected suppliers to be invited to tender)
* Subject one or more applying service providers (based on their responses to the information request) to a relationship assessment (if required) to verify that they do not pose a significant risk to SÜDVERS' information.

The security measures to be provided by external service providers must:

* be documented and approved by a sufficiently senior representative of the external service provider
* be set out in a contract and signed by an authorized person representing each party (e.g. SÜDVERS and the external supplier)
* are applied in practice and regularly monitored
* are subject to an audit or alternative security processes
* be checked regularly (at least once a year).

Contracts with external service providers and their subcontractors must contain agreed obligations and safeguards that specify the following:

* Compliance with national and/or international laws such as the GDPR or REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of December 14, 2022 on digital operational resilience in the financial sector (DORA) and the associated technical and implementation standards
* Compliance with international standards such as ISO 27001ff, ISO 27014, ISO 27017, ISO 27018, ISO 27036, ISO 27701, ISAE 3402 and ISO 22301.
* Requirements and obligations that SÜDVERS has assumed in contracts with other external parties (such as customers, clients and business partners)
* the need to obtain permission to outsource or share SÜDVERS information beyond the external service provider
* the need for the service provider's suppliers and subcontractors to meet the same safety requirements (often referred to as "flow-down clauses")
* the requirement for management and reporting of actual and suspected incidents
* the right to carry out penetration tests, evaluation and quality assurance
* the need for performance monitoring and reporting to identify and address non-compliance, poor performance, ineffective technical controls or incidents
* the right to audit the external supplier (and its suppliers), including the frequency and nature of the audit, or an agreement on alternative security procedures if an audit is not possible
* Requirements for the external provider to ensure that company data is protected at all times, even during and after completion of a service
* the need for them to provide regularly updated information on their ability to meet certain safety requirements
* the option to renegotiate the terms during the term of the contract (or at certain intervals) if the level of information risk changes
* an exit plan and the conditions under which SÜDVERS has a right of termination.

When signing a contract, the external service providers must:

* are recorded in a register (e.g. a service provider and contract database or an equivalent facility)
* identify a business owner, a contract manager, contacts from the procurement team (or equivalent) and information security.

The information security status of external service providers must be assessed/validated regularly (at least annually) according to a uniform and approved methodology (e.g. based on an industry standard) to ensure that key milestones are achieved and reports are submitted in accordance with the agreed criteria.

A uniform methodology for the exit, termination, renewal and renegotiation of contracts with external suppliers must be introduced, which includes the following:

* Establish a methodology to decide whether a contract should be terminated, canceled, extended or renegotiated (e.g. based on whether the impact of one or more major incidents was sufficient to recommend termination or cancellation of the contract to or whether the supplier has met the contract and evaluation criteria)
* Withdrawal of physical and logical access rights to SÜDVERS information
* the return, transfer or verified secure destruction of physical assets (e.g. backup media, documentation, hardware and authentication devices)
* compliance with license agreements and intellectual property rights
* Rehearsal and refinement of termination measures.
* When renewing or renegotiating contracts with external service providers, information security arrangements must be reviewed and revised information security terms proposed.

Alternative (contingency) arrangements must be in place to ensure that SÜDVERS' business processes can continue in the event that one or more external service providers are unavailable (e.g. due to contract termination, disaster, dispute with an external service provider or cessation of business by a service provider). These arrangements must be based on the results of a risk assessment and include the following:

* the provision of alternative, secure facilities for the continuation of business processes
* Deposit of information and closed/protected technologies (e.g. source code of applications and cryptographic keys) by a trusted external party, e.g. a legal representative, lawyer or equivalent person
* Recovery arrangements to ensure the continuous availability of information stored with an external provider or in the cloud
* Integration into the IT business continuity program of SÜDVERS.