

Security Policy   
IT BCM

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| IT Business Continuity 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, its majority-owned subsidiaries, and 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 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 | IT asset management is now dealt with in a separate asset management guideline | |

Table of contents

[1 Principles 4](#_Toc188864157)

[2 Objectives 4](#_Toc188864158)

[3 Controls 5](#_Toc188864159)

[3.1 IT business continuity strategy 5](#_Toc188864160)

[3.2 IT Business Continuity Program 6](#_Toc188864161)

[3.3 Reliable technical IT environments 8](#_Toc188864162)

[3.3.1 Maintenance of devices and equipment 10](#_Toc188864163)

[3.4 Information security in the event of a disruption to business continuity 11](#_Toc188864164)

IT business continuity and information security are complementary approaches to managing SÜDVERS' operational risks, and their objectives and focus often overlap. The goal of IT business continuity is to provide management with the assurance that critical business processes (whether automated or not) will continue to operate at an acceptable level, with a focus on the availability of information and infrastructure. Information security complements business continuity by providing management with assurance that information risks are managed within acceptable limits and ensuring that sensitive information is not disclosed to unauthorized parties and critical information is not tampered with.

# Principles

IT must define an IT business continuity strategy that promotes the need for IT business continuity management, embeds IT business continuity management in the general business continuity management of SÜDVERS and is implemented in the form of an IT business continuity program.

IT must establish a program for the continuity of IT operations that includes the development of a reliable technical infrastructure, the creation of crisis management capacities and the coordination and maintenance of plans and arrangements for the continuation of IT operations at SÜDVERS.

Critical business applications and the underlying technical IT infrastructure must run on robust, reliable hardware and software and be supported by alternative or redundant facilities.

# Objectives

Align IT business continuity objectives with SÜDVERS' business objectives, ensure resilience to disruptions and minimize the impact on SÜDVERS in the event of a disaster or emergency.

SÜDVERS is to be enabled to withstand a prolonged unavailability of critical information, business applications and the associated technical infrastructure and to provide employees with a series of documented measures to be implemented in the event of a disaster or emergency.

Ensure that critical business processes that rely on business applications and the technical IT infrastructure are available when needed.

# Controls

## IT business continuity strategy

IT must develop and maintain an IT business continuity strategy that is coordinated with the overarching SÜDVERS business continuity, IT and information security strategy.

The CEO must appoint a person who is responsible for IT business continuity at SÜDVERS.

An IT Business Continuity Management Team (or equivalent) must be established that:

* is responsible for the development, implementation and maintenance of the SÜDVERS IT Business Continuity Strategy and for the coordination with the general Business Continuity Strategy of SÜDVERS
* Responsible for and manages a program of IT business continuity activities

The IT business continuity strategy must be based on a solid understanding of SÜDVERS and take into account at least the following:

* SÜDVERS' risk appetite (e.g. the level of risk that SÜDVERS is prepared to accept/tolerate)
* the changes in threats and threat events faced by SÜDVERS (such as hacktivism, industrial espionage and denial of service attacks)
* Stakeholder requirements (e.g. to maintain business operations and to meet legal, regulatory and contractual requirements relating to business continuity)
* Requirements for protecting the integrity of information (e.g. against corruption) and the confidentiality of information (e.g. against unauthorized disclosure)
* key business environments (including the culture of local environments and the jurisdictions in which these environments operate), key business processes and products/services offered
* Agreements with external parties (e.g. customers, outsourced and cloud service providers and their suppliers).

The IT business continuity strategy must help to ensure at least the following:

* IT business continuity management is embedded in the overarching business continuity management of SÜDVERS
* critical business processes are supported by a robust technical IT infrastructure (e.g. by duplicating business applications, IT systems and networks and by eliminating individual sources of error)
* SÜDVERS is able to manage a major crisis (e.g. by maintaining crisis management and setting up a crisis team)
* IT business continuity planning is carried out as a formal work program
* Systems that support critical business processes can be restored within a predefined time frame
* Sensitive information (e.g. information that may only be disclosed to authorized persons) and critical information (e.g. information that must be available and whose integrity must be guaranteed) remain protected in the event of a disaster or emergency.

## IT Business Continuity Program

The IT business continuity management team must establish an IT business continuity program that supports the overall business continuity strategy of SÜDVERS.

The IT business continuity program must determine the individual business environments to be supported by IT business continuity plans and arrangements by identifying and documenting at least the following relevant details (e.g. in a business continuity risk register):

* the most important business areas and regions of SÜDVERS
* Critical business processes (in order of priority) and associated IT business applications
* the underlying technical IT infrastructure
* important internal and external interest groups.

Business owners must be appointed for each individual business environment, who are responsible for the corresponding IT business continuity plan and the corresponding precautions and are supported by a local team.

IT BCM plans and emergency scenarios must be defined for each individual business environment and tested at least once a year

The IT business continuity program must specify at least the following:

* the tasks and responsibilities of the persons involved in business continuity
* IT business continuity risk assessments are conducted for each individual business environment (including assessment of potential business impact, threats and vulnerabilities) to determine availability requirements
* the risk treatment options for maintaining business operations are identified and selected (e.g. accepting risks, avoiding risks, transferring risks or mitigating risks).

The IT business continuity program must apply to SÜDVERS as a whole and be binding for every business unit:

* follow the SÜDVERS crisis management process
* maintain contact with the SÜDVERS crisis management team
* Building resilient business applications and technical IT infrastructures (e.g. duplicate IT systems and networks) to support critical business processes and protect against targeted attacks, e.g. denial of service attacks
* develop and maintain comprehensive IT continuity plans for critical areas of SÜDVERS (e.g. based on an IT continuity risk assessment)
* Providing alternative arrangements to support critical IT business processes in the event of a major incident or disaster
* regular review and testing of IT business continuity plans and arrangements (including associated security controls) (e.g. as part of a business continuity exercise)
* keep the plans and arrangements for maintaining IT operations up to date.

The IT business continuity management team must maintain a central asset register for each individual business environment that includes at least the following:

* the results of the IT business continuity risk assessments (including details of key threats, threat events, availability requirements and risk treatment options selected)
* the plans for maintaining IT operations
* the details of the arrangements for IT business continuity
* the results of tests of IT business continuity plans and arrangements
* other important documents, such as IT business continuity awareness and training material, incident management plans, contracts and test plans.

## Reliable technical IT environments

Important or critical business processes must be supported by business applications and technical IT infrastructures that use robust, reliable hardware and software and are supported by alternative or redundant facilities.

The probability of important or critical business applications and the technical IT infrastructure failing must be reduced by taking the following measures:

* Use of hardware and software that is easy to maintain and can meet the requirements of critical business processes
* High priority on reliability, compatibility and capacity during the procurement process
* Ensuring compliance with general or industry-standard security standards for hardware and software
* Use of telecommunications network connections and services that have proven to be robust and resilient.

The availability of important or critical business processes must be improved by:

* Simultaneous execution of critical business applications at several locations (e.g. through hot standby or virtualization)
* Provision of alternative locations from which business applications, IT systems, networks and voice facilities can be operated and managed
* Automatic identification and recovery of transactions after a business application/system failure.

Important or critical business processes must be protected against interruptions caused by incompatible business applications:

* Running critical business applications on a dedicated physical or dedicated virtual server
* Support for critical business applications via a special network or subnetwork
* Prevent the transmission of information from connected systems that do not have acceptable security controls.

The reliability of important or critical business processes must be improved by reducing individual sources of error in the network:

* Automatic rerouting of network traffic in the event of failure of critical network devices or connections
* Installation of duplicate or alternative network devices (such as routers, firewalls, switches and Wi-Fi access points) for critical communications equipment
* Alternative connection points and connections to external service providers.

IT BCM and emergency plans must be drawn up for every IT system and every IT service and tested at least once a year. The results must be documented and the plans revised if necessary.

A complete IT-BCM test must be carried out at least once a year. The results must be documented and the plans revised if necessary.

The availability of communication services used to access external IT systems, networks and voice facilities (including those provided in the cloud) must be protected by the following measures:

* Provision of duplicate or alternative connection points to external communication carriers
* Forwarding of critical connections to more than one external exchange
* Agreement on the use of an alternative communication provider
* Setting up an emergency bypass for internal voice communication systems so that they can fall back on direct calls.

The resilience of the technical IT infrastructure must be improved by applying the usual maintenance and servicing measures, which include the following

* the maintenance of consistent software versions
* Maintenance of the devices according to the maintenance intervals recommended by the manufacturer
* the prohibition of maintenance of devices by unqualified persons
* Maintaining a sufficient supply of system consumables
* Ensuring that devices that support critical business processes or are particularly prone to failure can be replaced quickly (e.g. by keeping spare parts on site).

The reliability of the technical IT infrastructure must be improved by proactively initiating measures to rectify faults:

* Recording of all actual or suspected errors
* Deactivation of devices, software and services with suspected faults until these have been rectified
* Ensuring that critical IT systems, networks and voice communication systems are repaired or replaced within specified deadlines.

Critical business applications and the underlying technical IT infrastructure must be protected against targeted cyber attacks (e.g. denial of service attacks, hacking or targeted malware):

* Determining how the threat events affect the business environment in which the business processes take place
* Increased monitoring of critical business applications to prevent, detect or delay disruptions when they occur (e.g. denial of service attacks or repeated attempts to gain unauthorized access).

When implementing redundant important or critical IT systems, at least the following must be taken into account:

* Conclusion of contracts with two or more providers of networks and critical information processing facilities, such as Internet service providers;
* Use of redundant networks;
* Use of two geographically separate data centers with mirrored systems;
* Use of physically redundant power supplies or sources;
* Use of multiple parallel instances of software components with automatic load balancing between them (between instances in the same data center or in different data centers);
* Presence of duplicate components in systems (e.g. processor, hard disks, memory) or in networks (e.g. firewalls, routers, switches).

### Maintenance of devices and equipment

To prevent the loss, damage, theft or compromise of information and other related assets or the interruption of the organization's operations due to lack of maintenance, the following rules must be observed:

* Maintenance of the devices and equipment in accordance with the supplier's recommended service intervals and specifications;
* Implementation and monitoring of a maintenance program by the organization;
* Repairs and maintenance work on devices may only be carried out by authorized employees;
* Documentation of all suspected and actual errors as well as all preventive and corrective measures;
* Implementation of appropriate measures when devices and equipment are scheduled for maintenance, taking into account whether this maintenance is carried out by employees on site or by external parties. Obligation of maintenance personnel to sign a suitable confidentiality agreement;
* Supervision of maintenance personnel when carrying out maintenance work on site;
* If necessary, authorization and control of access for remote maintenance;
* Apply appropriate security measures for off-site assets when equipment containing information is taken off-site for maintenance;
* Compliance with all maintenance requirements imposed by the insurance company;
* Before recommissioning devices and equipment after maintenance, inspect them to ensure that they have not been tampered with and are working properly;

## Information security in the event of a disruption to business continuity

In the context of IT BCM planning and response to business continuity disruptions, it may be necessary to adjust information security requirements depending on the nature of the disruption compared to normal operating conditions. Here, the consequences of the possible loss of confidentiality and integrity of information must be considered and prioritized in addition to the need to maintain availability. Corresponding information security requirements must be included in the IT BCM processes and plans for maintaining or restoring the information security of business processes after a disruption or failure must be developed, implemented, regularly reviewed, revised and evaluated.

Once the disruption to business continuity has ended, the defined "normal level" of information security must be restored.