

Security Policy   
End user systems

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| End User Systems | |  |
| 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 | 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 Device configuration of the end user systems 4](#_Toc188861563)

[1.1 Principles 4](#_Toc188861564)

[1.2 Objectives 4](#_Toc188861565)

[1.3 Controls 4](#_Toc188861566)

[2 End user device connectivity 7](#_Toc188861567)

[2.1 Principles 7](#_Toc188861568)

[2.2 Objectives 7](#_Toc188861569)

[2.3 Controls 7](#_Toc188861570)

[3 Enterprise Mobile Device Management (EMM) 8](#_Toc188861571)

[3.1 Principles 8](#_Toc188861572)

[3.2 Objective 8](#_Toc188861573)

[3.3 Controls 8](#_Toc188861574)

[4 User responsibility for end user systems 10](#_Toc188861575)

[4.1 Principles 10](#_Toc188861576)

[4.2 Goals 10](#_Toc188861577)

[4.3 Controls 10](#_Toc188861578)

[5 Employee-owned devices (BYOD) 11](#_Toc188861579)

[5.1 Definition and delimitation 11](#_Toc188861580)

[5.2 Principles 11](#_Toc188861581)

[5.3 Objective 11](#_Toc188861582)

[5.4 Controls 11](#_Toc188861583)

# Device configuration of the end user systems

## Principles

End user devices must be created using standard technical configurations and be subject to security management practices to protect SÜDVERS information from unauthorized disclosure, loss and theft.

## Objectives

Ensure that end users' devices do not compromise the security of the information stored on or processed by them and, if the devices are lost or stolen, prevent unauthorized access to SÜDVERS information.

## Controls

End-user devices (including laptops and employee-owned devices) must be supported by documented standards/procedures that include the following:

* System configuration (e.g. firmware backup and use of standard builds)
* Provision of software to protect them (e.g. system administration tools, access control mechanisms, software to protect against viruses and malware as well as encryption functions)
* Protecting the memory of computing devices from attacks and misuse by malicious or compromised applications (e.g. by enabling DEP and using ASLR to prevent buffer overflow attacks)
* Use of encryption to protect sensitive information
* Configuration of the logging of security events based on the recommendations of the software manufacturers of the operating system and the applications used
* Access to the SÜDVERS networks.

The end devices must be equipped with standard configurations that include the following:

* Preconfigured BIOS (or similar) settings (e.g. deactivation of the boot menu, USB setup and DVD boot option, activated TPM chip)
* Restricting access to the BIOS functions (or similar functions) to a limited number of authorized persons, e.g. administrators (e.g. through password protection).

The end-user devices must be equipped with standard technical configurations that include the following:

* a standard operating system, trusted and approved applications, common communication software and security software
* Access control mechanisms (such as passwords, tokens or biometric data) to restrict access to the device to a limited number of users and administrators
* Measures to prevent the execution of unauthorized applications (e.g. by using whitelists or application execution tools that only allow certain authorized applications or blacklists that prohibit the execution of certain applications) in a trusted and secure environment
* Measures to prevent access to the device by unauthorized remote control software
* Deactivation of the "Autostart" function for devices other than the primary boot device (e.g. from CDs, DVDs, portable storage devices and mounted/shared network folders).

End-user devices must be configured to prevent the use of remote access software without the explicit and active consent of the user logged on to the end-user device. To strengthen this control, remote access must be

* be authorized by the user of the terminal device for each individual session
* be visible to the user of the terminal device at all times

End users' devices must be subject to standard security management practices that include the following

* Access to the system is granted according to the principle of least privilege
* Ensuring that they are kept up to date (e.g. by applying approved change management and patch management procedures)
* Maintenance of up-to-date malware protection software (including program code and signature files) to prevent infection by malicious software (such as computer viruses, worms, Trojans, spyware, rootkits, keystroke loggers, adware and botnet software)
* Use of a comprehensive set of system management tools (such as MDM solutions, maintenance programs, remote support, enterprise management tools)
* Option of backing up locally stored data that is located in defined directories
* Automatic blocking after a certain period of inactivity of maximum 15 minutes.

End-user devices must undergo system hardening that includes at least the following:

* Removal or restriction of unnecessary applications (e.g. unauthorized games, software and utilities not relevant to the company)
* Deactivation of unnecessary services (e.g. Telnet, Internet file sharing, FTP client) and user accounts (e.g. the "guest" account (or an equivalent account) for Microsoft Windows and UNIX systems)
* Changing the default passwords for administration
* Application of a technical hardening standard in accordance with the Information Security Directive.

End-user devices must take the following measures to protect the confidentiality of stored information:

* Use full disk encryption to protect (by default) all information stored on internal hard disks[[1]](#footnote-1) (or similar)
* Use file-based encryption features to protect individual files and folders (including files on portable storage devices and flash memory cards such as Secure Digital (SD)).

End-user devices used to access business applications over insecure networks (e.g., unsecured Internet connections) must protect sensitive information from unauthorized access (e.g., by unapproved or unauthorized applications) by preventing application information from being transmitted to the device in clear text (e.g., by using business applications via terminal servers (e.g., thin client) or web browsers that use an encrypted communication channel to the device).

End-user devices must be configured to log important security events (e.g. system crashes, unsuccessful logins by authorized users and unsuccessful changes to access rights).

End user devices that contain non-public SÜDVERS information and are not fully encrypted must be provided with a default configuration that allows the information to be remotely wiped once the device is reported lost or stolen.

# End user device connectivity

## Principles

End-user devices (including laptops and employee-owned devices), when not used in the corporate environment, must be equipped with secure procedures for connecting to other SÜDVERS systems and to SÜDVERS services and SÜDVERS networks.

## Objectives

Ensure that users' end devices are protected against unauthorized access and unauthorized disclosure of SÜDVERS information is prevented.

## Controls

End-user devices (including laptops and employee-owned devices) must have documented IT standards/procedures for connectivity that include the following:

* Prevention of unauthorized wireless access
* Protection against untrusted networks
* Setting up a virtual private network (VPN)
* Configuring web browsers
* the use of web proxy servers if the device is connected to internal SÜDVERS networks.

End-user devices must be protected from unwanted connections initiated by wireless networks and computing devices by restricting wireless connections such as Wi-Fi, 3G, 4G/5G/LTE, Bluetooth and Near Field Communication (NFC).

End devices that access the SÜDVERS network from remote environments must be configured in such a way that they:

* prevent access to unprotected networks while the device is connected to the corporate network
* split tunneling and bridging/routing

End-user devices that can connect to untrusted networks (including the Internet) must be protected by the following measures:

* Installation and maintenance of personal firewalls to restrict incoming and outgoing network traffic
* Activation of additional security-relevant
* Use of host-based intrusion prevention system software to detect unexpected application behavior and stop known attacks.

End user devices that require access to the internet (typically with web browser software) must use approved web browser software (to reduce the introduction of vulnerabilities associated with web browsers not supported by SÜDVERS)

The web browser software must be configured so that it:

* prevents users from disabling or changing the security options in the software settings
* limits the caching of information
* Pop-up window minimized
* enables web browsers to prevent the storage of authentication data such as passwords or tracking information by the browser.

# Enterprise Mobile Device Management (EMM)

## Principles

Smartphones, tablets and other devices with mobile operating systems (e.g. iOS and Android) and the applications ("apps") running on them must be protected in the event of loss, theft or cyber attacks by using an EMM system.

## Objective

The aim is to ensure that critical and sensitive information processed by people working with smartphones and tablets is adequately protected.

## Controls

An EMM system must be used to centrally manage and protect smartphones, tablets and the mobile applications they support.

The components of an EMM system that must be used on mobile devices include

* Mobile Device Management (MDM), which monitors, manages and protects the business-relevant information stored on smartphones and tablets
* Mobile Application Management (MAM), which provides, manages and protects mobile applications across different device types and operating systems

MDM functions that are used on mobile devices must include at least the following remote functions:

* Enforcing the use of PIN/passcode (e.g. requiring users to authenticate themselves each time they use the device by entering a four- or six-digit code)
* Blocking (e.g. to prevent unauthorized access to a lost or stolen device)
* Monitoring of device activity (in case evidence is needed for forensic analysis)
* Erase (often referred to as "remote wipe") to securely destroy all information stored on the device and any connected storage (e.g. flash memory cards such as Secure Digital (SD) and Compact Flash).

The MAM functions must be configured in such a way that they:

* Manage approved apps in a private company app store (e.g. a custom portal that offers a catalog of apps for download or a secure gateway to approved public app stores)
* restrict access to apps (e.g. depending on the function and type of device used)
* Deploy applications in an isolated, encrypted area on the device (e.g. in a container or sandbox)
* Support whitelisting or blacklisting of externally developed apps or app categories (e.g. based on a reputation analysis that examines the developer history and the type of information the app wants to access and share)
* Provide default configuration settings for applications (e.g. to fulfill predefined user-, group- or device-specific configuration requirements)
* enable the timely updating of applications (e.g. patches and maintenance of the latest version of installed applications).

# User responsibility for end user systems

## Principles

Information that is stored on, processed by or accessible via users' endpoint devices must be protected.

## Goals

Protecting information from the risks posed by the use of user endpoint devices.

## Controls

Users must observe the following principles when using their IT systems:

* Deregistration from active sessions and termination of services that are no longer required;
* Protect user endpoint devices from unauthorized use through a physical measure (e.g., key lock or special locks) and a logical measure (e.g., password access) when not in use; do not leave devices containing important, sensitive or critical business information unattended;
* the devices must be used with particular care in public places, open-plan offices, meeting places and other unprotected areas (e.g. confidential information must not be read if other people can read it from behind and privacy filters must be used);
* Physical protection of users' endpoint devices against theft (e.g. in cars and other means of transport, hotel rooms, conference centers and meeting places).

# Employee-owned devices (BYOD)

## Definition and delimitation

The abbreviation BYOD stands for Bring Your Own Device. It is a concept from the IT sector that allows employees of a company or members of an organization to use private end devices such as notebooks, smartphones or tablets to store or process business information.

For the purposes of this policy, BYOD use does not include the use of employee-owned devices to access company-owned terminal server infrastructures (e.g. Citrix Terminal Server) or to obtain/verify additional personal authentication information (e.g. MS Authenticator).

## Principles

If SÜDVERS permits the use of employee-owned devices (e.g. employee-owned tablets and smartphones) for business purposes, this must be supported by additional and documented agreements with the employees and by technical security controls to protect business information.

## Objective

Ensure that business information stored or processed on BYOD receives the same level of protection as when using company-owned devices (e.g. SÜDVERS laptops).

## Controls

The possibility of using BYOD must be approved by the management.

BYOD must:

* are classified as untrustworthy by default
* comply with a technical specification defined by IT (e.g. manufacturer and model of the device, operating system and required security features such as complex passwords and device encryption)

BYOD users must be engaged in a comprehensive and targeted security awareness campaign to help them understand and comply with acceptable use policies. The security awareness campaign must include regular communications to BYOD users covering the following points

* the risks associated with the use of BYOD
* the need to protect BYOD and the information stored on them

Access to SÜDVERS' networks and business applications must be restricted to approved BYOD devices that meet a minimum security configuration, including that the device is

* is registered
* is authenticated
* has not been manipulated ('jailbroken'),
* is operated with an approved and patched version of the operating system, i.e. the operating system version used must not be older than
  + the previous version for iOS devices
  + the two previous versions for Android systems
* is encrypted
* supports the remote updating of policies
* requires strong authentication
* is protected by a screen saver that is activated after 10 minutes of inactivity at the latest.
* is protected by an EMM system and
* has up-to-date protection against malware (including firewall, if technically possible).

Technical controls must be implemented to ensure the protection of business information on BYOD (throughout the lifecycle of each device) that include at least the following:

* Management and control of BYOD that can access business applications by SÜDVERS (e.g. by restricting access via a virtual private network (VPN), firewalls and proxy servers)
* the maintenance of a register (or equivalent document) of employees' approved devices by the IT department
* Restricting access to business information (e.g. through MCM, access controls and the separation of business and private applications and information)
* Protection of business information in the event of loss or theft of employee devices (e.g. through the use of mobile device management (MDM) software that is managed centrally)
* Creation and maintenance of configuration settings for application and device management (e.g. automatic updates of the operating system and applications)
* Configuration of employee-owned devices to log important security events (e.g. when sensitive information is copied to another device).

BYOD used to access business applications must protect sensitive information from unauthorized access (e.g. by unauthorized or unapproved applications) by:

* the storage of confidential business information on the device is restricted (e.g. through the use of business applications via terminal servers (e.g. thin client) or web browsers)

Users of BYOD are obliged to inform the IT helpdesk as soon as the device is no longer to be used for business purposes and to request the secure deletion of business content.

1. The solution used to encrypt the entire hard disk must ensure that the encrypted hard disks remain unreadable if the system is booted from another hard disk or another device. [↑](#footnote-ref-1)