Spreenauten.de
Spreenauten
Radio Technology (DMR, TETRA, ATEX, WLAN & 5G)
- DMR Radio Technology
- Two-way Radios
- TETRA Radios & Radio Cells
- Atex Radios
- Battery & Charging Technology for Radios
- Headsets & Loudspeaker Microphones
- WLAN - Wireless LAN as MESH-LAN & conservative WIFI
- DECT Phones & Repeaters (Base Stations)
- Tour Guide systems
- Antennas & Antenna Technology
- 5G

Motorola & Hytera
Service
Radio technology
Applications

Spreenauten GmbH
Meeraner Str. 11b
12681 Berlin. Germany

Fon
+49.(0)30.293.8197-0
Freecall Internationl
00800.11.88.44.00
Fax
+49.(0)30.293.8197-0
E-mail
support@spreenauten.com
Website
www.spreenauten.de
HRB
AG Berlin-Charlottenburg
136729B
UST-ID Deutschland
DE279088233

Executive Summary Information Security

The information security policy of Spreenauten GmbH describes how confidential information is effectively protected at Spreenauten GmbH. Due to the constantly changing IT threat scenario, weekly training and updates for our team are a top priority. The current status of the Information Security Policy should therefore be understood as a basis, but not as a comprehensive description of our information security.

Object

The objective of all our information security measures is to protect our information against access by third parties and disclosure in the best possible way and in accordance with the current state of the art.

Definition of information

Information is all knowledge that comes within our scope. It is irrelevant how this happens. This includes conversations (e.g. in meetings) as well as files of any kind and knowledge of processes relating to our company and our business partners.

Confidentiality

We do not distinguish between confidential and other information, but assume that all information is shared exclusively with individuals (and never with groups of people) who absolutely need this information for their work in our company and who have been granted the appropriate security clearance by us.

Responsibilities

Information security is one of the highest principles at Spreenauten GmbH. This means that every employee is responsible for maintaining information security in their area and has a duty to report any breaches.

Contact Information security

Information security & data protection officer: Nico Ludvikova
privacy@spreenauten.com

CTO: Daniel Knappe dk@spreenauten.com

[Updated 25 May 2025]

Information security through protective processes

Process

Processes describe how information is handled in our company. They are clear instructions and define, with regard to the information security of Spreenauten GmbH, which employees work with which information and how it is handled. They are subject to ongoing adjustments, e.g. to new risk scenarios, and are internalised by our employees in regular training sessions. Their effectiveness and application are tested in audits and simulated attacks.

(Information) protection processes

Spreenauten GmbH protects information within its sphere of influence through the strict application of preventive and protective processes that go far beyond the underlying guidelines (-> 2.11). These can be found in the document ‘Protective

processes of Spreenauten GmbH (C)'. This document is a resource that is only available to the relevant employees of Spreenauten GmbH. They are not disclosed to third parties. In this case, disclosure would not weaken the security measures we have taken, but would allow a potential attacker to consider how to circumvent them.

The following sub-items therefore refer to general best practice, which we naturally also apply:

Social engineering – countermeasures (think first)

Spreenauten GmbH is aware of the danger posed by social engineering and recognises it as one of the most important risk scenarios for its data protection. We therefore consider training and maintaining the awareness of our employees to be the most important countermeasure. We do this both automatically through regular surveys, which are an integral part of our HR system, and in regular employee appraisals. We check the effectiveness of these measures through regular simulated attacks.

See also 'IT Security Spreenauten GmbH (p. 16, paragraph 2, Attacks / Social Hacking' (C).

Storage of information

Less is more. Spreenauten GmbH only stores information that is absolutely necessary for processing orders and maintaining business relationships. No further information is stored.

Information is stored in encrypted form. The storage location and information are protected by effective access controls.

See 'Storage and access control of information at Spreenauten GmbH' (TS).

Sharing information

Information is only made available to other employees if they need it to process an order. The only exception to this is information relating to company-wide projects. Internal information silos must always be avoided.

If information must be passed on for compelling reasons, this is done exclusively to individual employees and never to group distribution lists. The basis for this is the document 'Guidelines for the internal disclosure of information at Spreenauten GmbH' (C).

If information must be passed on externally for compelling reasons, this shall only be done on the basis of the 'Guideline on the external disclosure of information by Spreenauten GmbH' (C). Furthermore, the basis for the external disclosure of information is that compliance with paragraph 4 (subsidiarity) of this document is ensured.

Deletion of information

Spreenauten GmbH only retains information for as long as is necessary for the processing of an order, the maintenance of a business relationship or for legal reasons.

If none of these reasons apply, the information is deleted. Physical information carriers (e.g. files, DVDs) are destroyed in accordance with DIN 66399 in compliance with security level 4.

Digital information carriers (HD, SD, etc.) are deleted in accordance with the 5220-22-M standard of the US Department of Defence.

Details are regulated by the work instruction ‘Data protection-compliant deletion of information’ (C) of Spreenauten GmbH.

The current COO of Spreenauten GmbH is responsible for compliance with this point.

Password security

Information stored digitally by Spreenauten GmbH is encrypted and protected with secure passwords or keys.

The systems we use enforce secure passwords. Access data is stored in encrypted apps (so-called password safes). Password changes are enforced by the system at close, but deliberately irregular, intervals.

See also ‘IT Security Spreenauten GmbH: Basics - Focus: Device’ page 3, paragraph 2 ‘Password security’.

Handling information processing technology

Spreenauten GmbH regularly trains all employees in the safe and careful use of information processing technology. In addition to the password security mentioned above, there is a focus on social engineering (e.g. phishing) and the danger of technical attacks (e.g. Trojans and RAM software attacks). The focus is on correct behaviour, recognising risks, the correct application of defensive techniques and the correct reporting of security problems or incidents.

The current Information Security & Data Protection Officer at Spreenauten GmbH is responsible for this. Further details on the handling of information processing technology can be found in the document ‘IT Security Spreenauten GmbH: Basics - Focus: Devices’ (C).

Clean Desk Policy (CDP)

Spreenauten GmbH considers the ‘Clean Desk Policy’ to be one of the most effective processes for protecting information.

Compliance with this policy is checked daily. This applies to workplaces (office, warehouse, technical facilities) as well as conference rooms and company cars.

Further details are regulated by the ‘Clean Desk Policy of Spreenauten GmbH’.

The current information security and data protection officer is responsible for implementation and monitoring.

Access protection

Spreenauten's premises are protected by several coordinated systems and processes. Access authorisation and access denial are granted on an individual basis. File and server rooms require at least 3-factor identification and authentication. Physical access is never granted to an employee alone, but always in the company of another person. The accompanying person is determined automatically and at random.

Underlying guidelines

Spreenauten GmbH bases the design and implementation of protective processes on

Spreenauten GmbH bases the design and implementation of protective processes on the following guidelines:

ISO/IEC 27001

Information technology – Security techniques – Information security management systems – Requirements

BSI Standard 200-1

Management Systems for Information Security

Internal audits

Regular internal audits, which are either enforced automatically via our HR system or take place in face-to-face meetings, ensure that all employees are aware of the need for processes that protect information within our scope and that they apply them correctly.

External audits

In addition, protective processes and their application are reviewed by external companies. In this context, our basic assumptions regarding information security in our company are also reviewed.

Information security through technical protection

Systems

All data-processing technology that we use in our company, including workstations, laptops, servers and smartphones, routers and switches, as well as IoT devices such as printers, scanners and barcode scanners.

This also includes radio equipment and repeater technology. The latter are also fully subject to our information security policy.

System protection

Spreenauten GmbH protects the systems it uses through the strict application of technical protection and defence measures that go far beyond the underlying guidelines (-> 3.6). These are explained in the document ‘System protection of Spreenauten GmbH (TS)’.

Office IT hardware

Office IT hardware refers to all local systems that our employees use for information processing in the course of their work for Spreenauten GmbH. This includes PC systems, printers, barcode scanners, smartphones and all IoT devices used by us. In addition to the information security policy set out here, the regulations contained in the document "IT Security Spreenauten GmbH: Fundamentals – Focus: Devices‘ (C).

Application security

The hardware and software developed by us is based on our ’General Security Concept of Spreenauten GmbH for the Development of Hardware and Software" (S) and on a security concept that is individually tailored to the functionality and environment in which the hardware or software is used. This extended security concept is created together with the customer and is a central component of regular audits. The current CTO is responsible for reviewing the security concepts for the hardware and software we develop, which in turn must be reviewed by the current information security and data protection officer.

Radio technology

The radio technology we rent, sell, install, design, develop or manufacture is fully subject to our information security policy. In the field of radio technology, this policy is governed by the document ‘Work instructions for securing radio technology provided to customers by Spreenauten GmbH.’ (S) These work instructions are binding for all employees who design, produce, install or provide radio technology for our customers. Their validity and implementation are closely monitored in internal audits by our QA department. Security deficiencies are reported directly to the current Information Security & Data Protection Officer. However, our QA department remains responsible for ensuring that defective technology does not enter the goods traffic.

Updates & patches

Security-related updates and patches for the systems we use are installed immediately after release. However, this must be done within 2 hours (365/24/7) at the latest. The current CTO and, on his behalf, IT OPS are responsible for this.

The installation of updates and patches, as well as the responsibility for this in the case of wireless technology provided, sold or installed by us, is regulated individually in the respective support agreement.

In general, we inform our customers immediately after publication, but no later than 2 hours after we become aware of a relevant update or patch.

Central management

The systems we operate are managed and administered centrally.

The details of our system administration are regulated by the document ‘System Administration of Spreenauten GmbH’ (TS - IT) and the instructions based on it.

Monitor

Our systems are continuously monitored ‘live’. This is done automatically by standardised systems, e.g. as part of our network monitoring, as well as by security routines developed in-house that report any anomalies.

Our system monitoring is staffed 24/7 by two employees with extensive authorisations, including the power to shut down the system.

If live monitoring is not possible for technical reasons, the logs are read at regular intervals on site.

Underlying guidelines

The following guidelines apply to information security at Spreenauten GmbH:

GDPR (EU)

Cybersecurity Act (USA)

BSI Standard 200-3 Risk analysis based on IT

See also:

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679

https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf

pdf

Our measures for securing information far exceed these guidelines. Nevertheless, we consider them to be the minimum requirement for information security in a company and are happy to demonstrate their fulfilment at any time.

As the USA and the EU are different legal jurisdictions, the directive that requires the stricter data protection applies in each case.

Internal audits

The review of the measures we have taken with regard to the information security of our system is a central component of the monthly system protection audit. The current CTO of Spreenauten GmbH is responsible for this. Furthermore, we use automated surveys (knowledge checks) to ensure that our employees have internalised the purpose of the measures and the corresponding instructions for action and apply them.

External audits

Audits by external companies enable us to test our information security system under real conditions (white hat/black hat). If security deficiencies are identified, they are tested and rectified by us immediately.

Subsidiarity Information security

Customers

To protect our customers, our employees and our company, we expect our customers to comply with basic standards in the area of information security.

This includes, among other things, the careful handling of data, continuous system-wide checks for malware and the use of secure technology for sharing and making data available.

When working on site, we also require basic network security, such as encrypted and protected WiFi.

If problems arise, we address them directly with our customers. If no solution can be found and we classify the risk scenario as threatening to us, we reserve the right to reject orders for this reason.

We have defined the minimum standards for our customers in the document ‘Information & IT Security Policy for Customers of Spreenauten GmbH’.

Suppliers

We expect a high level of information security from our suppliers. This includes a complete information security protocol as well as, for example, the option of fully encrypted communication with AES 256 as a minimum standard.

If these requirements are not met, we will discuss this with our suppliers. If no solution can be found, we reserve the right to terminate the business relationship or limit it to areas where no extended exchange of information is necessary.

We have defined the standards we require from suppliers in the document ‘Required standards of Spreenauten GmbH for suppliers’ (C). The information security standards can be found in paragraph 3.

Service providers

The present information security policy of Spreenauten GmbH applies without exception to all our service providers.

Violations of this policy will always result in the immediate termination of the service contract.

Authorities

We consider the information security situation at public authorities to be critical. We only pass on information relating to third parties to public authorities if this is explicitly requested by our customers – e.g. when applying for frequencies on behalf of customers. For this purpose, we use only the original interfaces of the respective authority. Classified data of classes TS, S and C is not passed on to public authorities. Should this nevertheless become necessary, the written approval of the current CTO AND the current CEO of Spreenauten GmbH is required.

Information security & data protection training

In order to ensure the implementation and effectiveness of our information security policy and the fundamental guidelines affected by it, we train our employees regularly and check the success of this training through internal and external audits.

The training is the responsibility of the respective supervisors. It takes place on a monthly basis. The current Information Security & Data Protection Officer of Spreenauten GmbH is responsible for checking that the training takes place.

The current CTO of Spreenauten GmbH is responsible for checking the success of the training.

The procedure, frequency and objective of the training are regulated individually for each employee in our HR system.

Reporting violations and problems

We encourage our employees, suppliers and business partners to report any problems relating to our information security at any time. We have set up an IT-based system for our employees, which they can use to suggest improvements and report problems with just one click. We have also implemented an attractive bonus system for this purpose.

The contact person for this is the current Information Security & Data Protection Officer.

Whistleblowing

Whistleblowers have the option of passing on information anonymously within the company. We have set up an IT-based system for this purpose, which effectively protects the identity of the sender and guarantees anonymity. Spreenauten GmbH also guarantees every whistleblower comprehensive protection against internal reprisals.

The contact person for this is the current Information Security & Data Protection Officer. He or she will also keep the identity of the whistleblower anonymous, insofar as this is known to him or her.

Problems and violations of our data security will be dealt with immediately and,

depending on the severity and complexity, resolved within a maximum of 2 weeks. In case of doubt, the Spreenauten GmbH emergency plan for information security issues will come into effect. This allows us to partially or completely deactivate our systems and processes globally in order to protect the information within our scope.

This emergency plan can be found in the document ‘Spreenauten GmbH emergency plan for information security issues’ (S).

Monitoring of the information security policy

Strict compliance with the information security policy, including its sub-items, is continuously monitored, reviewed and updated as necessary.

The current information security and data protection officer is responsible for this.

Any improvements required will be implemented as quickly as possible.

Employees are encouraged to provide feedback on this policy if they have suggestions for improving it. Feedback of this kind should be addressed to the current Information Security & Data Protection Officer.

Changes to this policy

This policy is not part of an employment contract with an employee of Spreenauten GmbH, but it is a work instruction. Spreenauten GmbH may amend it at any time to update or improve information security within your company.

Severability clause

Should individual provisions of this policy be or become invalid or unenforceable, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision that comes as close as possible to the objective (information security) pursued by the invalid or unenforceable provision. The above provisions shall apply mutatis mutandis in the event that the policy proves to be incomplete.