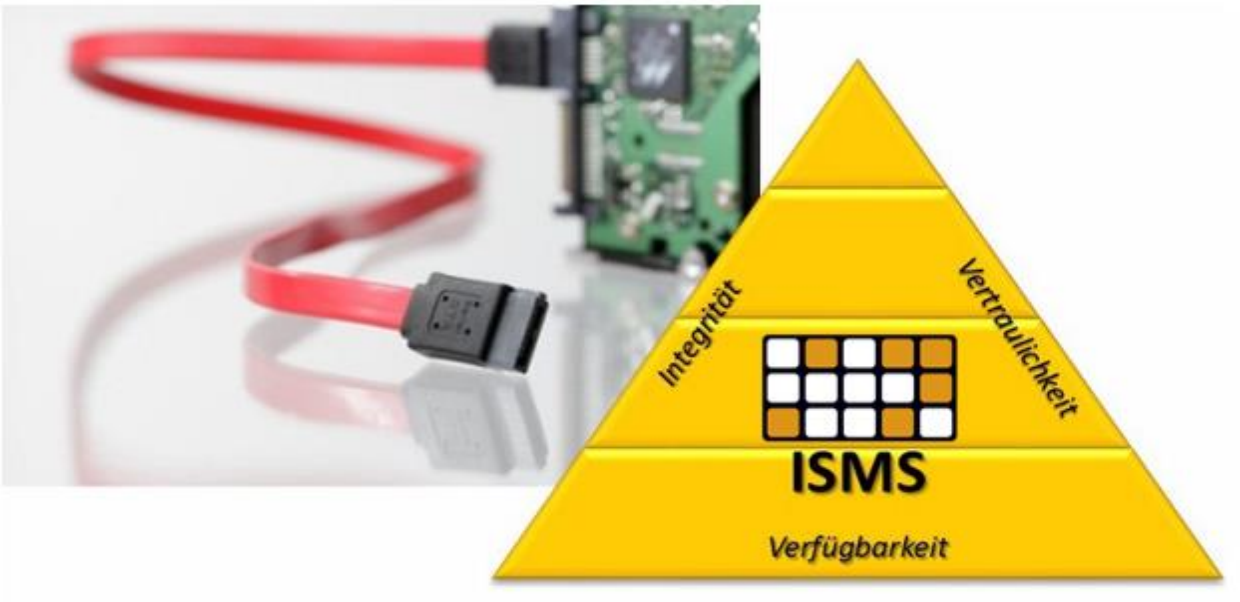


Guideline for Partner Companies

Guideline of e.solutions Information Security

Autor: Ostermeier Caroline; Brauns Benjamin

Translation: Automatically translated and quality inspection by Brauns Benjamin

Version: 2.4

Status: RELEASED

Valid from: 02.04.2024

ISMS classification: public

Legal Notice: The English version of this guideline is for informational purposes only and is provided “as is”. In the event of ambiguities, the German version shall prevail.

The document is invalid as printed.

The latest version can be found at:

https://sharepoint.esolutions.de/sites/pub_infosec/SitePages/Home.aspx and

https://b2b.esolutions.de/informationsecurity.html

Table of Contents

1 Document information

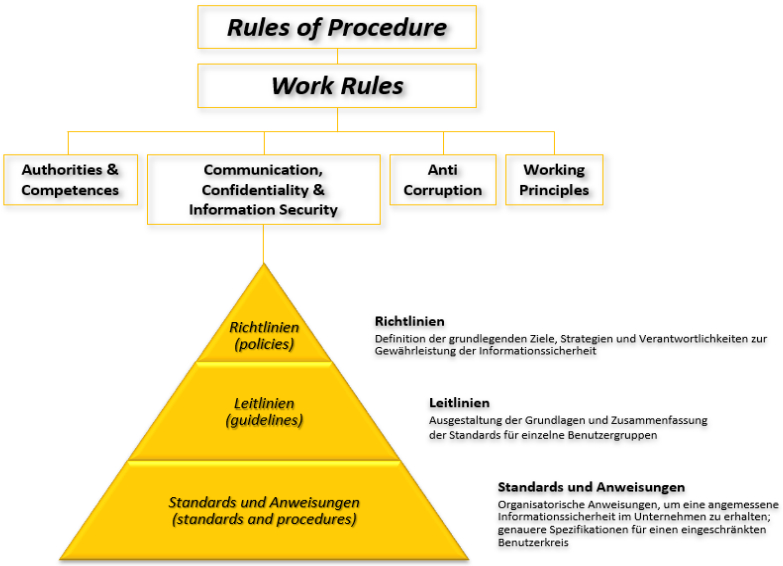
1.1 Document history

Date	Rev.	Editor	Description	changed pages/chapters
01.11.2018	0.9	J. Pfannenstein	Initial version of the document	
15.11.2018	1.0	J. Pfannenstein	Preparation Review	
29.01.2019	2.0	J. Pfannenstein	Update	Policy Pyramid and IS
09.07.2019	2.1	P. Walhekar	Adaptation to references Adding no private use of e.solutions work equipment	Chap. 8 Chap. 9.1
12.11.2019	2.2	P. Walhekar	Adjustment of the backup regulation	Chap. 10.1.4
03.02.2021	2.3	C. Ostermeier	Adaptation to new layout and update	
13.07.2021	2.4	B. Brauns	Author change Add chapter, target group, knowledge transfer and appendix Corrections to content Comparison of the specifications with the ISMS manual	Chap. 2, 9.6 and 13
06.09.2021	2.4	B. Brauns	Automatically Translated by translation engine and QA	
11.03.2022	2.4	C. Ostermeier	Update Links	Complete Document
02.04.2024	2.4	C. Ostermeier	Adaption of footer; Rainer Lange removed from management	

1.2 Classification

This document is a guideline of e.solutions GmbH. The document is to be treated confidentially. It may only be used and distributed according to the document classification “public”.

1.3 Context



1.4 Responsibilities

The persons responsible for this guideline are:

- CISO, e.solutions GmbH
- Information Security, e.solutions GmbH

1.5 Competent authorities within the meaning of the guideline

1.5.1 Organization and compliance

- Named contact persons in the commissions
- Legal department of e.solutions
- Data protection officer of e.solutions
- Information security of e.solutions

1.5.2 Technology and issues

- B2B Support[1] of e.solutions
- e.solutions CERT[2]

2 Target group

This guideline *must be* read and observed by **persons** in partner companies[3] who **provide services for e.solutions GmbH** on the basis of contractual regulations. Furthermore, the guideline *must be* read by **persons** within e.solutions GmbH which **are responsible for or affected by the cooperation with partner companies** in their area of responsibility and/or duties.

[1] https://b2b.esolutions.de/support.html

[2] eso.Group.CERT@esolutions.de

[3] Definition of partner company withinin chapter 4

3 Preliminary remarks

The "Guideline for Partner Companies" serves to protect the confidentiality, integrity, availability and traceability of information as well as the rights and interests of e.solutions GmbH and all natural and legal persons who maintain a business relationship with us.

4 Key Message

The Guideline for Partner Companies defines the information security regulations to be observed by partner companies in their area of responsibility for IT systems & applications and infrastructure provided and used by them.

Partner companies must identify and comply with applicable regulations.

This guideline defines the information security rules to be followed by partner companies when handling information and IT devices (e.g. PCs, workstations, laptops, smartphones or tablet PCs).

Partner companies are defined in this guideline as any third party that provides services for e.solutions on the basis of contractual relationships. e.solutions acts here as the "client" of the partner companies.

This guideline for action is addressed to the management of the partner companies, their employees, Fulfillment/Delivery Agents and Affiliates (collectively referred to herein as "Contractors").

The purpose of the information security policy is to protect the confidentiality, integrity and availability of information and to protect the rights and interests of the contracting authority and all natural and legal persons who enter into a business relationship with the contracting authority and/or carry out activities on its behalf.

5 Scope

The guidelines apply to the partner companies of e.solutions GmbH and are to be applied in the entire partner network for partners who provide services for e.solutions GmbH on the basis of contractual regulations and to be structured by concrete organizational and technical regulations (e.g. IT regulations) in individual cases.

6 Implementation

The rules are independently mandatory.

Furthermore, managers are responsible for the correct implementation of and compliance with this guideline.

If individual regulations can’t be implemented in the current situation (e.g. for technical reasons), proceed as follows:

- The circumstance must be reported to the information security team
- In individual cases, everyone must behave in such a way as to come as close as possible to the actual aim and purpose of the regulation.

In case of compelling need, deviating exceptions may be approved in writing by the Information Security Team.

7 Validity

This guideline is valid indefinitely and without restriction as long as it is not replaced by a more recent version.

8 Applicable documents

All other documents of the information security organization of e.solutions GmbH apply internally to e.solutions.
In addition to this guideline, the contracts concluded apply to the partner companies. Should the partner company gain access to the client's information systems, the special regulations for these systems shall also apply.

8.1 Initial provision of documents to partner companies

As part of the contract initiation process, the future partner company receives the following documents

- from the B2B-portal[4] of e.solutions
- or by the legal department of e.solutions GmbH

8.2 Provision of updated documentation to partner companies

Partner companies are required to check regularly if there are any updated documents. The partner company can always view or download the current versions of the documents applicable via the B2B portal[5].

Rules from updated documents are to be implemented immediately by the partner company.

9 General requirements

The following requirements must be met by all partner companies, regardless of their specific assignment and regardless of the specific form of cooperation. Requirements for the client are not part of this document.

9.1 Organizational requirements

With regard to bringing IT equipment onto the company premises or into security areas of the Client that are not provided by the Client, the Client's regulations shall apply.
The private use of work equipment provided by the Client (e.g. ePN.Client) is prohibited.
The use of data or software belonging to the Client on IT systems or storage devices which are neither provided nor released by the Client or the Contractor is not permitted.
The transfer of data to third parties is only permitted with the written approval of the Client's data owner.
Regulations of the Client on the collection, processing and use of personal data must be complied with.

[4] https://b2b.esolutions.de

[5] https://b2b.esolutions.de/informationsecurity.html

Employees of the Contractor must be bound by their management to maintain confidentiality in accordance with the existing non-disclosure agreement (NDA) between the Client and the Contractor. The Client shall be granted access to these agreements at any time.
If the Client's data is stored on mobile systems or IT devices, these shall be encrypted using state-of-the-art hardware or software.
Before travelling abroad, the country-specific regulations on the use of safety techniques (e.g. encryption) must be observed.
After the end of the contract, all data of the Client must be handed over to the Client and must be demonstrably deleted from all devices and storage media of the Contractor. Legal requirements (e.g. storage obligations) must be observed.

9.2 Personnel security

A user ID that is no longer required or an access right for data of the Client that is no longer required must be reported immediately by the respective user to the respective commissioning authorities (e.g. responsible user administrator of the Client) so that the corresponding blocking/deletion can take place. If it is a user ID within e.PN[6], the partner company administrator must delete it immediately within the B2B portal.
Identification media that are no longer required (e.g. smartcards, SecurID cards) must be returned to the ordering party without delay.
Any equipment (e.g. laptops) and data carriers or storage media provided must be returned to the Client at the end of the contract or when they are no longer required.
The loss of IT devices handed over to the user of the Contractor as well as of media for the purpose of authentication must be reported immediately by the user to the competent authority of the Client.

9.3 Physical and environmental security

IT devices that store or process data of the Client shall be used in such a way that no unauthorized persons can view or access such data. Particular care should be taken when using mobile systems. Confidential and highly confidential documents must never be left unattended to prevent access by unauthorized persons.

9.4 Management of organizational values

9.4.1 Rules for classification

Classification takes place on the basis of the three protection goals confidentiality, integrity and availability and must be carried out for all information and all information-processing IT systems.
The Contractor must request the classification according to confidentiality, integrity and availability (within the scope of the contracts) from the Client.
Information shall be protected from unauthorized access throughout its lifecycle in accordance with measures appropriate to its confidentiality classification. Confidentiality classifications can be assigned an expiration date.

[6] e.solutions Partner Companies Network

If necessary, the classification with regard to integrity, non-repudiation and availability shall be checked and determined by the respective process owner when processing data. This classification shall be evaluated regularly, with the involvement of the information owner, and adapted if necessary.

The correct classification must be confirmed by the information owner.

9.4.1.1 Confidentiality

Information which is not intended for the general public may only be made accessible to those persons who are entitled to it (principle of "need-to-know").

The following classification levels are defined in relation to the **confidentiality** of information:

Classification	Definition
öffentlich / public	Information that is not subject to any restrictions and can be published, for example, in the press or on the Internet. The use of company information in public is subject to the approval of the competent bodies. Examples: Homepage, social media, company presentations
intern / internal	Information whose knowledge by unauthorized persons, improper disclosure or use has only a minor influence on the achievement of product and project goals and therefore may be made accessible to an authorized group of people. Breaches of confidentiality can have negative consequences, albeit of a rather minor nature. Example: Claims for damages by individuals or organizations are unlikely to be successful Examples: Customer/supplier addresses, delivery notes, invoices, protocols, notices, memos, process descriptions, employee phone list, layout, policies, work rules, health and safety documents, project/process data
vertraulich / confidential	Information disclosure to an unauthorized person can and may endanger the company from product and project goals, may and therefore only be made accessible to a limited group of authorized persons. Confidentiality breaches are likely to result in measurable negative consequences, such as: ▪ Loss of customers ▪ Decline in sales/turnover figures ▪ Claims for damages by individuals or organisations Examples: Employment contracts, warnings, cancellations, personnel data, personal data, price lists, calculations, quotations, contracts, orders, business analyses, bank account data, time management, payroll accounting, customer specifications, source texts, software, targets (pre-series and series parts), design images (e.g. 3D models of cars, at customer request), project and process data (at customer request)
streng vertraulich / strictly confidential	Information disclosure to unauthorized persons can greatly jeopardize the achievement of corporate objectives and must therefore be made available only to an extremely restrictive distribution list and be subject to strict controls. Confidentiality breaches have a significant negative impact on the image or appearance of the company as well as economic consequences, such as: ▪ Substantial loss of customers ▪ Sharp decline in sales/turnover ▪ Claims for damages by various individuals or organisations ▪ Exclusion from certain market areas

Classification	Definition
	▪ Negative effects in the public perception Examples: Design drawings of prototypes

9.4.1.2 Integrity

The error-free processing of information and protection against unauthorized changes must be ensured.

The following classification levels are defined in relation to the **integrity** of information:

Classification	Definition
gering / low	A breach of integrity has no foreseeable impact on the business activities or the image or appearance of the company.
mittel / medium	A breach of integrity has only a minor impact on the business activities and/or the image or appearance of the company. There may be negative consequences, albeit on a small scale. Examples: ▪ Slight delays in work processes ▪ Errors without impact on work results (no productive downtime) ▪ Decisions are not affected ▪ Claims for damages by individuals or organisations are unlikely to be successful Examples: Location maps, organizational charts, individual internal phone numbers
hoch / high	A breach of integrity has a tangible impact on the business activities and/or the image or appearance of the company. There are likely to be measurable negative consequences, such as: ▪ Loss of customers is likely ▪ Decline in sales/turnover figures likely ▪ Significant delays in workflows ▪ Faults/malfunctions with perceptible effects on work results (high production losses) and/or failure of some service processes ▪ Decisions are affected/ wrong decisions are likely ▪ Claims for damages by individuals or organisations are likely Examples: JIT orders, press releases, website content, production control data
sehr hoch / very high	A breach of integrity will have a substantial impact on the company's business operations and/or image or appearance, as well as corresponding consequences, such as: ▪ Substantial loss of customers ▪ Claims for damages by various individuals or organizations ▪ Sharp decline in sales/turnover ▪ Exclusion from certain market areas ▪ Significant delays in workflows ▪ Faults/malfunctions with serious effects on work results and/or failure of several service processes (very high productive downtimes) ▪ Decisions are strongly affected / wrong decisions Examples: Accounting (e.g. financial statements), cryptographic keys, salary

9.4.1.3 Availability

Information must be available within an agreed period of time.

The following classification levels are defined in relation to the **availability** of information:

Classification	Definition
gering / low	The availability of the IT system must be less than 95 % in terms of failure or unacceptable response times, without any significant damage (financial or to the image of the company). Example: Intranet application with general employee information
mittel / medium	The availability of the IT system shall be at least 95 % in terms of failure or unacceptable response times. Lower availability leads to measurable damage (financial or to the company's image). Example: Applicant portal; internet presence
hoch / high	The availability of the IT system shall be at least 98 % in terms of failure or unacceptable response times. Lower availability leads to significant damage (financial or to the company's image). Examples: Payroll, accounting
sehr hoch / very high	The availability of the IT system shall be at least 99 % in terms of failure or unacceptable response times. Lower availability leads to substantial damage (financial or to the company's image). Example: IT system whose failure results in an immediate stop of the work processes Significant impairments may include: ▪ Loss of customers ▪ Claims for damages by various individuals, organisations or associations ▪ Sharp decline in sales/turnover ▪ Exclusion from certain market areas ▪ Faults/malfunctions with serious effects on work results and/or failure of several service processes (very high productive downtimes)

9.4.2 Labeling scheme

Requirements for information creators and owners:

- Newly created information and data must be marked by the creator.
- The information owner is responsible for the classification.
- The creator must request the correct classification via the information owner.
- Confidentiality classifications must be made for all IT systems.
- If a classification is not yet clear, for example in the case of newly created documents/IT systems, the classification "confidential" should be selected.
- The information owner must check (at the latest whilst next review or update) for internal, confidential and strictly confidential information whether its confidentiality classification is still correct and mark it accordingly.

Specifications for the recipient:

- Unmarked information and data are considered "confidential".

- In case of doubt about the classification, the information owner should be contacted.

Information may only be made available to an authorized group of persons for the purpose of the agreed activities and in compliance with the relevant regulations. The "need-to-know" principle must be followed.

Information must be protected from unauthorized access throughout its lifecycle according to its current confidentiality classification.

The following rules apply:

Classification	Requirements
öffentlich / public	▪ Labelling: none/optional (e.g. note in imprint) Reproduction and distribution: no restrictions ▪ Storage: no restrictions ▪ Deletion: no restrictions ▪ Disposal: no restrictions
intern / internal	▪ Marking: on all pages of the document within footer with "intern" or "internal". ▪ Duplication and distribution: only to authorized employees of e.solutions GmbH and authorized third parties within the scope of the activity or the area of application. ▪ Storage: Protection against unauthorized access ▪ Deletion: Data that is no longer required must be deleted ▪ Disposal: proper disposal
vertraulich / confidential	▪ Marking: on all pages of the document within footer with "vertraulich" or "confidential". ▪ Duplication and distribution: only to a limited group of authorized employees of e.solutions GmbH and authorized third parties within the scope of the activity and the scope of application. The person distributing the information is responsible for appropriate distribution methods to protect the information and data from unauthorized access and/or eavesdropping (e.g. using encryption). ▪ Storage: Access only for a limited group of authorized employees of e.solutions and authorized third parties within the scope of the activity as well as the scope of application (e.g. by closed user groups). Suitable storage locations and/or storage media shall be used. ▪ Confidential documents must be stored in locked steel furniture or in locked rooms that can only be opened by a group of persons authorized to do so when they are not required. ▪ Deletion: Data that is no longer required must be deleted. ▪ Disposal: proper disposal ▪ Authentication: Strong authentication ▪ Transport: Confidential documents and storage media must be sent in sealed, neutral envelopes; if necessary, the words "personal" can be added. This means that the envelope may only be delivered directly to the named recipient.
streng vertraulich / strictly confidential	▪ Marking: on all pages of the document in the footer with "streng vertraulich" or "strictly confidential" In addition, all pages must be marked with "page x of y". ▪ Duplication and distribution: only to an extremely limited group (e.g. list by name) of authorized employees of e.solutions GmbH and authorized third parties within the scope of the activity or application and after prior

Classification	Requirements
	approval by the information owner. As far as technically possible, all data shall be encrypted in accordance to the current state of the art. If this is not possible, comparably strong security solutions must be used. Depending on the use case, further technical or organizational protective measures must be used (e.g. Prohibition of forwarding and printing, watermarks). Suitable media that prevent eavesdropping (e.g. encrypted video conferences) must be used for communication. ▪ Storage: Access only for an extremely limited group (e.g. list of names) of authorized employees of e.solutions and authorized third parties within the scope of the activity as well as the scope of use case (e.g. by closed user groups). As far as technically possible, all data shall be encrypted in accordance with the current state of the art. If this is not possible, comparably strong security solutions must be used. ▪ Strictly confidential documents must be stored in locked steel furniture. Separate locks must be used for this purpose. Mobile data carriers with strictly confidential information must be stored in suitable data safes. ▪ Deletion: Data that is no longer required must be deleted. ▪ Disposal: proper disposal ▪ Authentication: strong authentication ▪ Transport: strictly confidential documents and storage media must be sent in neutral, sealed outer envelopes (without additions such as "personal, strictly confidential, etc."). A second inner envelope, marked "strictly confidential", containing the strictly confidential documents, shall be placed in this envelope.

The requirements for handling information (labelling, copying, distribution, storage, deletion and disposal) also apply to IT systems (e.g. databases and backup media). Stricter legal requirements (e.g. data protection requirements) remain unaffected.

9.4.3 Knowledge sharing

All conversations (including telephone calls, video and web conferences) involving or containing confidential or strictly confidential information shall be protected from unauthorized interception.

Fax numbers and e-mail addresses must be taken from current directories or requested from the recipient in order to avoid incorrect transmissions.

For the transport of IT equipment and data carriers outside the Client's building or premises boundaries, the Client's regulations and company agreements shall be binding.

The sender is responsible for the content and distribution of an e-mail. For further processing and distribution of recipients.

The creation and sending of chain emails is not permitted.

9.4.4 Handling of storage and recording media

Data carriers (such as CDs, DVDs, USB sticks and hard disks) must be protected against loss, destruction and mix-up as well as unauthorized access.

Data carriers that are no longer required must be disposed of in a safe manner.

9.5 Information security incident handling

Information security incidents (e.g. occurring malfunctions, breaches of the information security regulations) which affect data or systems of the Client must be reported immediately to the competent body.

Suspected vulnerabilities and weaknesses of IT systems shall be reported immediately to the competent body. The testing of vulnerabilities and weaknesses (e.g. penetration testing) may only be carried out by the competent body.

In case of suspicion of loss of confidential or highly confidential information, this must be reported immediately to the competent body (see chapter 1.5).

9.6 Distribution of knowledge

The Contractor must ensure in an appropriate manner, on a regular basis, that the contents of this guideline are communicated to the persons within his organization who work for the Client. At best, this must be supported by evidence.

9.7 Compliance and adherence to legal obligations

The partner company must set up a compliance management system that considers legal and operational requirements (including resource management, internal control system, IT continuity management and protection of information). This must include all information, hardware and software of the Client.

Compliance management must include the following.

9.7.1 Early risk detection

A process for early detection of risks and potential threats to IT systems and data must be implemented.

Preventive activities and measures must be taken to address identified risks.

9.7.2 Intellectual Property / License Management

All intellectual property rights (e.g. Copyrights to software, documents and graphics, design rights, trademarks, patents and source code licenses) must be observed and complied with.

The use of unlicensed software (pirated copies) is not permitted.

Licensed software is subject to copyright laws (e.g. making copies, except for backup and archival purposes, is a violation of copyright laws).

Violations of these provisions may result in criminal prosecution and may result in injunctions or claims for damages.

Licensed software may only be used for the agreed purpose in compliance with applicable regulations and license agreements with the manufacturer.

9.7.3 Data protection

The respective country-specific laws and regulations on data protection must be complied with.

Contractor[7] must be obliged by the management of the respective partner company to comply with the statutory data protection requirements.

9.7.4 Contractual compliance

The IT organization of the partner company must meet the contractual requirements of the Client. Measures must be implemented to ensure that the partner company's own organizational regulations are reviewed and kept up to date so that the current contractual requirements are depicted.

9.7.5 Internal rules and regulations

Partner companies must provide their employees with regulations and principles of conduct to ensure compliance with the requirements and the appropriate handling of information as well as hardware and software of the Client.

9.8 Infringements and enforcement

Violations of the information security guidelines must be examined and punished individually in accordance with the applicable operational, contractual and legal regulations and agreements.

10 Additional requirements for Contractor with direct access to the Clients information systems

The following requirements must be complied with by all partner companies that have access to information systems and thus information that is managed at the Client. It does not matter on which technological way or with which system this access is established.

10.1 Requirements

10.1.1 Internal organization

Partner companies may only provide or initiate the provision or installation of hardware and software via the department of the Client responsible for them.

With regard to the use of the hardware and software provided, the regulations and company agreements of the Client apply.

Opening the IT device and making changes to the hardware (e.g. assembly/ disassembly of hard disks, memory modules) as well as manual changes to the security settings (e.g. browser settings) is only permitted to the responsible authorities.

The use or subsequent modification of the Client's programs is only permitted if approved by the relevant authorities.

Only data that is necessary within the scope of the assignment is permitted to be processed on the IT equipment provided.

The systems provided may not be used for other Clients.

[7] Sub-contracting arrangement to pass on the commitment to data protection compliance.

The use of IT equipment or data of the Client by employees of the partner company requires the explicit consent of the Client. The Client is authorized to prohibit access or use at any time (e.g. in the event of misuse).
Data of the Client must be separated from data of third parties and especially from data of other Clients of the partner company (e.g. via rights management). Data must not be accessible to third parties (e.g. through encryption).
The e.solutions classification must be mapped to the partner company's classification scheme to ensure that all required security measures are implemented.
Partner companies must map the information security requirements from the set of rules handed over to them for the fulfilment of the task by means of appropriate security measures in their own company.
Access to data of the Client may only be granted to employees of the partner company according to the need-to-know principle.

10.1.2 Physical and environmental security

The equipment provided must be handled properly and protected from loss or unauthorized modification.
The manufacturer's instructions for protecting the equipment must be observed.

10.1.3 Protection against malware and mobile code

If malware is suspected, affected IT devices and data carriers must not be used any longer. The competent body must be notified immediately.

10.1.4 Backup

Data should be stored on the assigned network drives and not on the local hard disk, because only in the network a central and automatic data backup is guaranteed.
e.solutions IT is not responsible for the backup of data that is not stored on central network drives (e.g. local hard disk, mobile data carriers) or systems with comparable functionality.
Backup data and media for backup must be treated in the same way as the original data.

10.1.5 Access control

The following requirements are to be followed by all users:

- The use of another person's user ID or account is not permitted.
- The disclosure in means of identification (e.g. SmartCards or SecurID cards) is not permitted.
- Passwords or PINs of a user ID are intended for personal use (referred to as "personal user ID") must be kept strictly confidential and must not be disclosed.
- Storing or writing down passwords (e.g. on paper, via mobile devices or in files) is not permitted unless this is specified as a secure method.
- As soon as there is a suspicion that a password or PIN has been compromised or has become known (by other persons), it must be changed immediately.
- Temporary passwords (e.g. for new accounts) must be changed the first time you log in.

- All passwords or PINs must be changed the first time they are used and after one year at the latest (the latter only applies to passwords).
- The spying of passwords is not permitted.
- Passwords must be classified at least as confidential.
- If passwords must be kept in writing, they shall be kept by the employee in a sealed envelope in a suitable place protected from unallowed access (e.g. a safe). Each time a change is made, the stored password must be updated accordingly. The sealed envelope must be signed by the respective employee. The persons authorized to open the envelope must be named, as in exceptional cases (e.g. in the event of illness) it may be necessary to use the stored password. The so-called "two-person rule" must be followed. Each opening shall be documented and reported to the employee. After each opening, the employee must immediately change the password and store it again securely. As an alternative, IT systems are permissible which guarantee corresponding functionality (e.g. electronic password safes).
- When leaving the system during operation (e.g. break, meeting), the user must activate a system lock (e.g. password-protected screen saver).
- Users who use their multifunction badge to log on to IT systems must remove the badge from the reader when leaving the system.

10.1.5.1 Generation of passwords

The following minimum requirements must be met when generating a password:

- Employees (of the Contractor) are not permitted to use an identical password for professional and private purposes to access the Client's systems.
- Employees (of the Contractor) are not permitted to use an identical password for systems provided by the Client and systems provided by third parties (e.g. applications, registration services on the Internet).
- The minimum length enforced by systems for passwords must be adhered to. It shall be governed by the provisions of the relevant regulation.
- Trivial passwords (e.g. "Test123456") or passwords with a personal reference (e.g. names, date of birth) are not permitted.
- If certain systems or applications require more complex passwords (as defined in the password policy), then these requirements must be met.
- Note: For a secure password, you can use mnemonic devices or abbreviations as well as spoofs (example: "Every day I go to the bathroom and wash thoroughly" becomes the password "EdIgttb&wt").
- Alternatively, a combination of four words (e.g. "SunWoodTeaTime") creates a very strong password that is easy to remember. The examples given here must not be used as actual passwords.

10.1.5.2 PINs for unlocking smartphones and tablets

The requirements described in chapter 0 apply.

10.1.5.3 PINs for authentication smart cards

The requirements described in chapter 0 apply.

10.1.5.4 Group IDs

Group IDs are not permitted.

10.1.6 Access control for networks

An IT device provided by the customer may only be connected to networks outside the company (e.g. Hot Spot, private WLAN; except mobile networks) if this is done to connect to the e.solutions network. Direct "surfing" etc. is not allowed (except for smartphones and tablets connected to mobile networks).
If the connection is no longer required, it must be disconnected.
Unrestricted connections of communication devices (e.g. without firewalls) to the internal network (intranet) are only permitted if these are provided by the Client.

11 Handling of material requiring protection

Within the scope of the commissioning, material/components/samples may be handed over to the partner company by the Client which are subject to an increased protection requirement. For this material the rules from chapter 0 apply accordingly.
In addition to this, further guidelines can be handed over with the material, which are to be fulfilled additionally by the partner company.

12 Final provisions

Deviations from these guidelines that lower the security level are only permitted temporarily and after consultation with the competent bodies and the Client.

13 Appendix

References to the need for the document

The documents from the information security management system consider, among other things, the general protection goals of information security confidentiality, integrity and availability as well as the "need-to-know" principle. In addition, there are requirements from the VDA ISA catalogue that have to be fulfilled.

This document, together with the applicable documents from Chap.8 Response to the following controls of the VDA ISA Catalogue[8] in its version valid at the time of writing:

- Control Chapter 1.1.1: Existence of information security policies
- Control Chapter 6.1.1: Information Security at Contractors and Cooperation Partners

[8] cf. www.vda.de