Guideline

Security guideline for partners

Contents

0. Preface

0.1. Purpose of this document

The rules for information security, with which service providers must comply when handling information and IT equipment, are provided in this Information Security Guideline.

Service provider means any third party that provides a service to ALTEN on the basis of a contractual relationship.

These security guidelines are intended for management at the service provider company, its employees and its vicarious agents/agents (hereinafter referred to as the Contractor).

0.2. Scope

These guidelines apply to all service providers that provide services to ALTEN GmbH, ALTEN SW GmbH and ALTEN Austria Süd GmbH – hereinafter referred to as ALTEN, ALTEN Group or Client – in line with contractual agreements.

0.3. Document structure

Chapter	Target group	Comments
1	All service providers	All service providers are required to comply with the requirements set out in this chapter. Additional requirements are set out in Chapters 2 and 3. They require compliance depending on the access possibilities to the company network and the company systems.
2	Service providers with access to the company network or to company systems	In addition, the requirements of Chapter 1 must be complied with. If the service provider has access to the customer network and to customer systems, it must also follow the customer guidelines.
3	Service providers without access to the company network or company systems	In addition, the requirements of Chapter 1 must be complied with.

1. General requirements

The following requirements must be complied with by all service providers, in accordance with the definition supplied in this document.

Requirements for the Client are not part of this document.

1.1. Organisational requirements

Any rules of the Client relating to bringing IT equipment that does not belong to the Client onto the company premises or into security restricted areas (project offices) must be complied with.

The disclosure of data to third parties is permitted only with the written approval of the data owner of the Client.

Any rules of the Client relating to the use, storage and any type of processing of personal data (see also Appendix A.1.2) must be complied with.

Employees of the service provider must be obliged by their management to maintain confidentiality in the sense of the existing confidentiality agreement between the Client and the Contractor. The Client must be permitted to inspect such agreements at any time.

If client data is to be stored on mobile systems or IT equipment, it must be encrypted with state-of-the-art hardware or software.

On termination of the agreement, the client data must be handed over to the Client and must be erased on equipment and storage media of the service provider. The specifications of the Client and any legal requirements (e.g. confidentiality agreement, framework agreement, retention obligations) must be observed.

1.2. Personal security

A user ID or access authorisation to client data that are no longer required must be reported by the user without delay to the relevant commissioning office (e.g. user administrator responsible or client IT support, see A.1.4), so that the necessary blocking and erasure can be carried out.

Identification media that are no longer required (e.g. RSA tokens) are to be returned without delay to the commissioning office.

Any equipment (e.g. laptops) and data carriers or storage media provided must be returned to the Client on the expiry of the agreement or when they are no longer required.

The loss of IT equipment provided to the user and of media for the purpose of authentication is to be notified by the user to the relevant office of the Client (see Appendix A.1.4).

1.3. Physical and environment-related security

IT equipment that stores or processes client data is to be used in such a way that unauthorised persons cannot view or access the data. Particular care is required when using mobile systems.

Confidential and secret documents must never be left unattended, in order to prevent unauthorised persons viewing them.

1.4. Management of in-house values

1.4.1. Rules for classification

Classification is carried out on the basis of the three protection objectives of confidentiality, integrity and availability, and must be implemented for all information and all information-processing IT systems.

The purpose of this classification is to allocate a level to information, regardless of the protection needs. Different protection measures will be required depending on this classification.

Information (protection objective confidential) is to be protected from access by unauthorised persons for the entire duration of its life in accordance with the measures that relate to its confidentiality classification. When processing data, the classification in relation to integrity and availability should be determined by the relevant

process owner, if necessary. This classification should be regularly evaluated with the involvement of the information owner and where necessary revised.

1.4.1.1 Confidentiality

Information that is not intended for the general public must only be made accessible to persons who are authorised to access it (principle: on a “need-to-know” basis).

Specifications for author and owner of information:

- New information and data are to be labelled by the author.
- The information owner is responsible for the classification.
- The author has to request the correct classification from the information owner.
- All IT systems must be assigned to a confidentiality classification level.
- Where a classification level is not unambiguous, for example, in the case of newly entered documents/IT systems, the level “confidential” is to be selected.
- The information owner must (at the latest by the next review or update) check whether the confidentiality classification of internal (C1), confidential (C2) and strictly confidential (C3) information is still correct and label it accordingly.

Specifications for the recipient:

- Unmarked information and data are deemed to be confidential.
- If in doubt regarding classification, contact the information owner.

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

Classification	Definition
Public (C0)	This relates to all information that has been published by ALTEN and is therefore freely accessible, such as: • Advertising material (flyers, etc.) • All public areas on the website In the case of advertising material (flyers, etc.), the information does not have to be labelled.
Internal (C1)	This relates to all information, the unintended disclosure of which or its disclosure to a third party may cause damage to the company. This generally includes information that is accessible by a larger group of employees but not by external parties, such as: • Internal communication (correspondence by email, virtual teams), • Internal rules and regulations (guidelines, memos, instructions, organisational charts), • Internal information (work results, plans and intentions), • Publications on the intranet

Confidential (C2)	This relates to all information the unintended disclosure of which or the disclosure to a third party may cause considerable financial damage to ALTEN, may have legal consequences or damage the reputation of ALTEN. This information is always to be labelled “confidential”. This generally includes all information that is significant for the technical or financial success of individual departments. In particular, this includes all information that could be of particular value to competitors, such as: • Confidential communications (client correspondence by email, video conferencing & collaboration), • Ensuring competitiveness (marketing data, client and supplier data, customer queries), • Personal data, • Travel expenses and wage slips, • Research data, • Project information (commercial, technical), • Technical data (construction drawings of sensitive areas, network plans)
Strictly confidential (C3)	This relates to confidential commercial information the unintended disclosure of which or the disclosure to a third party may result in serious damage to the business purpose and objectives of ALTEN, serious legal consequences or serious damage to the reputation of ALTEN. This type of information is always to be labelled with the protection class “strictly confidential”. This usually includes information that is hugely important for the success and the continued existence of the entire company, such as: • Company strategies, • Technical and strategic planning, • Information about planned company acquisitions or company divestments, • Economic and budget plans from different departments, • Information from business partners that has the same level of confidentiality, • Information about crisis situations, • Copies of information that is strictly confidential

1.4.1.2 Integrity

The error-free processing of information and the protection against unauthorised revision must be ensured.

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

Classification	Definition
Low	An integrity breach has no foreseeable effects on the commercial activities or the image or the appearance of the company.
Medium	An integrity breach has only a minor impact on the commercial activities and/or the image or the appearance of the company. There may be negative consequences, even to a limited extent. Examples: • Small delays with workflow processes • Errors that do not impact work results (no productive downtimes) • Decisions are not impacted • Claims for damages by individuals or organisations are unlikely
High	An integrity breach has a noticeable effect on the commercial activities and/or the image or the appearance of the company. It is likely that there will be measurable negative consequences, for example: • Loss of customers is likely • Clear delays in workflow processes • Errors/malfunctions with discernible effects on work results (high level of production downtime) and/or disruption to some service processes • Decisions are impacted / incorrect decisions are likely • Claims for damages by individuals or organisations are likely
Very high	An integrity breach has a considerable effect on the commercial activities and/or the image or the appearance of the company and corresponding consequences, for example: • Significant loss of customers • Claims for damages by individuals or organisations are unlikely • Exclusion from certain market regions • Clear delays in workflow processes • Errors/malfunctions with a serious effect on work results and/or disruption to a number of service processes (very high level of production downtime) • Decisions are strongly affected / incorrect decisions are made Examples: Accounting (e.g. annual report), patents, cryptographic keys, salary statements

1.4.1.3 Availability

Information must be available within an agreed period of time.

The following classifications have been defined in relation to the availability of information:

Classification	Definition
Low	The availability of the IT system in terms of disruption or unacceptable response times may be less than 95%, without this resulting in significant impairment (e.g. of a financial nature or to the image of the company).
Medium	The availability of the IT system in terms of disruption or unacceptable response times must be at least 95%. A lower level of availability will lead to significant impairment (e.g. of a financial nature or to the image of the company).
High	The availability of the IT system in terms of disruption or unacceptable response times must be at least 98 %. A lower level of availability will lead to significant impairment (e.g. of a financial nature or to the image of the company).
Very high	The availability of the IT system in terms of disruption or unacceptable response times must be at least 99%. A lower level of availability will lead to significant impairment (e.g. of a financial nature or to the image of the company). Example: Where disruption to an IT system results in an immediate production stop A significant impairment can be, for example: • Loss of customers • Claims for damages by various individuals, organisations or associations Errors/malfunctions with a serious effect on work results and/or disruption to several service processes (very high production downtimes)

1.4.2. Labelling information and handling information

Information may only be made accessible to an authorised group of people for the purpose of the agreed activities and in compliance with the relevant regulations. The principle of the “need-to-know” is to be adhered to here.

Information must be protected from access by unauthorised persons for the entire duration of its life in accordance with its current confidentiality classification. The following guidelines apply:

Classification	Requirements
Public	The company’s internal specifications on the position of the classification label apply: • **Label**: “Public” (possible to do without label on flyers or other marketing measures) • **Reproduction and distribution:** no restrictions • **Storage:** no restrictions • **Erasure**: no restrictions • **Disposal**: no restrictions

Internal (C1)	The company's internal specifications on the position of the classification label apply: • **Label:** Details of the confidentiality level in the language of the country / "internal" on each page of the document in electronic and print format. • **Reproduction and distribution:** only to authorised employees of the company and authorised third parties, within the framework of the activity or the scope of application. • **Storage:** Protection from unauthorised access • **Erasure:** Data that is no longer required is to be erased (see Appendix A.1.2, A.1.3) • **Disposal:** proper disposal (see Appendix, A.1.2, A.1.3)
Confidential (C2)	The company's internal specifications on the position of the classification label apply: • **Label:** Details of the confidentiality level in the language of the country / "Confidential" on each page of the document in electronic and print format. • **Reproduction and distribution:** only to a limited group of authorised employees of the company and authorised third parties within the framework of the activity and of the scope of application. The person distributing the information is responsible for reasonable distribution channels in order to protect the information and data from unauthorised access and/or unauthorised eavesdropping (e.g. using encryption). • **Storage:** Access only for a limited group of authorised employees of the company and authorised third parties within the framework of the activity and of the scope of application (e.g. by means of a closed user group). Appropriate storage locations and/or storage media are to be used. • **Erasure:** Data that is no longer required is to be erased (see Appendix A.1.2, A.1.3) • **Disposal:** proper disposal (see Appendix, A.1.2, A.1.3) • **Authentication:** Strong authentication (2nd factor) • **Transport:** Confidential documents and storage media must be shipped in sealed, neutral envelopes; where necessary, the word "personal" may be added. This means that the envelope may only be handed directly to the named recipient.
Strictly confidential (C3)	The company's internal specifications on the position of the classification label apply: • **Label:** Details of the confidentiality level in the language of the country / "Strictly Confidential" on each page of the document in electronic and print format. In addition, all pages are to include the text "page x of y". • **Reproduction and distribution:** only for an extremely limited group (e.g. list of names) of authorised employees of the company and authorised third parties within the framework of the activity or the scope of application and after prior consent by the information owner. Where technically feasible, all data is to be encrypted in accordance with the state of the art. Where this is not possible, comparably strong security solutions are to be used. Depending on the type of application, further technical or organisational protection measures are to be taken (e.g. prohibition on forwarding and printing, water mark) • **For communication:** appropriate media are to be used that prevent eavesdropping (e.g. encrypted video conferences). • **Storage:** Access only for an extremely limited group (e.g. list of names) of authorised employees of the company and authorised third parties within the framework of the activity or the scope of application (e.g. based on closed user groups). Where technically feasible, all data is to be encrypted in accordance with the state of the art. Where this is not possible, comparably

	strong security solutions are to be used. • **Erasure:** Data that is no longer required is to be erased (see Appendix A.1.2, A.1.3) • **Disposal:** proper disposal (see Appendix, A.1.2, A.1.3) • **Authentication:** Strong authentication (2nd factor) • **Transport:** Strictly confidential documents and storage media must be shipped in neutral, sealed envelopes (without adding words such as "personal", "secret", etc.) A second envelope is to be placed within the envelope, and is to be marked with the classification level "secret" or "strictly confidential".

Unlabelled information that is clearly not "public" is to be classed as "confidential".

The specifications for handling information (labelling, reproduction, distribution, storage, erasure and disposal) apply equally to IT systems (e.g. databases and backup media).

1.4.3. Handling storage media

Data carriers (such as CDs, DVDs, USB sticks and hard drives) are to be protected against loss, destruction and a mix-up and against unauthorised access.

Data carriers that are no longer required are to be disposed of in a safe manner (see Appendix A.1.3).

1.4.3.1 Exchanging information

It is important to ensure that all conversations (including telephone calls, video and web conferences) that involve or contain confidential or secret information cannot be overheard without authorisation.

In order to avoid incorrect transmission, current directories should be checked for fax numbers and email addresses or these should be checked with the recipient.

The sender is responsible for the content and the distribution of an email. The recipient is responsible for further processing and distribution.

1.5. Handling information security incidents

Information security incidents (e.g. disruption, breach of information security legislation), that concern the data or systems of the Client, must be notified without delay to the relevant office (see Appendix, A.1.5).

Suspected vulnerabilities and weaknesses of IT systems must be reported without delay to the relevant office (see Appendix, A.1.4)

If a loss of confidential or secret information is suspected, this must be reported without delay to the relevant office (see Appendix, A.1.7).

1.6. Compliance and complying with statutory obligations

The service provider must set up a compliance management system having regard to legal and company requirements (including resource management, internal control system, IT continuity management and protection of information). It must include all information, hardware and software of the Client.

The relevant office (see Appendix, A.1.7) is to be contacted in the event of queries and for support. The compliance management system must contain the following:

1.6.1. Early risk detection

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

Preventative action and measures must be taken to deal with the recognised risks.

1.6.2. Intellectual property / licence management

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

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

For licensed software, the statutory provisions apply with regard to copyright (e.g. where making copies is in breach of copyright, with the exception of copies made for backup and archiving purposes). A breach of these provisions may result in criminal prosecution and an interim injunction or a claim for damages.

Licensed software must only be used for the purpose agreed and in compliance with applicable legislation and licensing agreements with the manufacturer.

1.6.3. Data privacy

The relevant country-specific legislation and provisions on data privacy (see Appendix A.1.8) are to be complied with.

Contractors must be obligated by management at the relevant service provider to comply with the statutory data privacy legislation.

1.6.4. Contractual compliance

The IT organisation of the service provider must meet the contractual requirements of the Client. Measures must be taken to ensure that the service providers own organisational regulations are reviewed and kept up to date, so that the current contractual requirements are included.

1.6.5. Internal instructions

Service providers must specify the regulations and code of conduct to their employees in order to ensure compliance with requirements and appropriate conduct when handling the information and the hardware and software of the Client.

1.7. Breaches and enforcement

A breach of the information security guidelines must be individually examined and penalised in line with the applicable corporate, contractual and statutory provisions and agreements.

2. Additional requirements (network access to the internal company network)

2.1. Definition

The following requirements must be complied with by all service providers that belong to one of the following categories:

- Clients (end equipment) are provided by ALTEN
- The connection is, for example, via VPN solutions with direct access to the ALTEN network and/or those of the customer.
- The connection is directly via the ALTEN network and/or that of the customer

These service providers may just as much be located on their own company premises as on the grounds of an ALTEN facility or of the customer.

2.2. Requirements

2.2.1. Internal organisation

Regarding the use of the hardware and software provided, the rules and works agreements of the relevant company apply.

Opening IT equipment and making changes to the hardware (e.g. installing/removing hard drives, memory modules) and manually changing the security settings (e.g. browser settings) is permitted only by the relevant department (see Appendix, A.1.4).

The use or subsequent change of programs of the Client is only permitted where it has been approved by the relevant department (see Appendix, A.1.4).

Data from other customers must not be processed using the IT equipment provided.

The use of client software or data on IT or storage equipment that has not been provided by the Client or that is not the Client's property is not permitted.

The use of client IT equipment or data by employees of the service provider requires the express permission of the Client. The Client is entitled at any time to prohibit access or use (e.g. in the case of misuse).

2.2.2. Physical and environment-related security

The equipment provided must be handled appropriately and must be protected from loss or unauthorised modification.

Equipment provided by the Client (e.g. laptops, mobile phones) may only be taken away with the prior permission of the Client.

2.2.3. Protection from malware and mobile program codes

If an attack from malware is suspected, the IT equipment and data carriers concerned must no longer be used. The relevant department (see Appendix, A.1.4) is to be notified without delay.

2.2.4. Backup

Data should be stored in the allocated network drives and not on a local hard drive, the reason being that a central and automated data backup is only guaranteed in the network.

The user is responsible for the backup of data that is not stored on central network drives (e.g. local hard drive, mobile data carriers).

Backup data and media for backing up are to be treated as the original data.

2.2.5. Access control

2.2.5.1 User responsibility

The following instructions are to be followed by all users:

- The use of the user ID or account of another person is not permitted.
- Passing on means of identification (e.g. smart cards, RSA tokens) is not permitted.
- The password or PIN of a user ID intended for personal use (referred to as "personal ID"), must be kept secret and must not be passed on to another person.
- As soon as there is a suspicion that a password or a PIN has been compromised or become known , they should be changed without delay.
- Temporary passwords (e.g. for new accounts) are to be changed at the first login.
- All passwords or PINs are to be changed the first time they are used and at the latest after 90 days.
- It is prohibited to spy out passwords.
- Passwords should be classified at least as confidential.

If passwords have to be stored in writing, they should be stored by the person responsible in a sealed envelope and in an appropriate location that is protected from unauthorised access (e.g. in a safe).

Each time it is changed, the stored password is to be updated accordingly. The sealed envelope is to be signed by the relevant employee.

The people who are entitled to open the envelope must be listed by name, as it may become necessary to use the stored password in exceptional circumstances (e.g. illness). In doing this, the “two-person-rule” should be followed.

Each time the envelope is opened it must be recorded and the person responsible notified. After each opening, the person responsible must change the password without delay and store it again securely.

As an alternative, IT systems are permitted that guarantee a similar functionality (e.g. electronic password safes).

When exiting a system during operation (e.g. break, meeting), the user must activate a system lock (e.g. password-protected screen saver).

2.2.5.2 Generating passwords

When generating a password, the following minimum requirements must be met:

- The password must have at least 10 characters including at least three of the following 4 types of character:
  - Upper case letters
  - Lower case letters
  - Digits
  - Special characters
- If certain systems or applications require more complex passwords, then these specifications are to be met.
- In particular, trivial passwords are not permitted (e.g. “Test1234”) or passwords that include a personal reference (e.g. name, date of birth).
- Employees (of the Contractor) are not permitted, when accessing the client systems, to use an identical password for professional and personal purposes.
- Employees (of the Contractor) are not permitted to use an identical password both for systems that have been provided by ALTEN and systems that have been provided by third parties (e.g. applications, registration services on the internet).

2.2.6. Access control for networks

2.2.6.1 Rules for using network services

IT equipment provided by the Client must only be connected to an external network (e.g. hotspots, private WLAN) if and for as long as this is necessary to create a connection with the company network (via remote access/VPN).

Once the connection is no longer required, it should be disconnected.

2.2.6.2 Equipment identification in networks

Unlimited connections of communication equipment (e.g. without a firewall) to the internal network (intranet) are only permitted if they are provided by the Client.

3. Additional requirements (without direct access to the internal company network)

3.1. Definition

The requirements set out in Chapter 3 must be complied with by all service providers that belong to one of the following categories:

- Service providers that do not have direct access to the network of a group company
- Service providers that are not provided with end devices that belong to an ALTEN company and only use end devices that belong to the company of the service provider.
- Service providers that are not connected via remote access or some other VPN solution.

These service providers are located on their own company premises and are subject to the rules and regulations of their own company.

3.2. Requirements

3.2.1. Internal organisation

The data from group companies must be separated from the data of third parties and especially from the data of other customers of the service provider (e.g. by means of rights management). Data must not be accessible by third parties (e.g. to be implemented by means of encryption)

The ALTEN information classification must be included on the classification diagram of the service provider in order to ensure that all necessary security measures are implemented.

Service providers must display the information security requirements drawn from the rules and regulations given to them in order to carry out the task, by means of appropriate security measures in their own company.

Access to client data may only be granted to employees of the service provider on a need-to-know basis.

4. Obligation to comply

This rule is to be complied with by all service providers in accordance with the definition in this document.

Should there be, in exceptional cases from this guideline, then it is only temporary and is permitted after consultation with the relevant departments (see Appendix A.1.5 - A.1.7) and the Client.

Appendix A

Specific characteristics are set out in this chapter that apply to a company.

A.1.1 Each Contractor is responsible for ensuring that the information, programs and IT equipment are only employed and used for corporate purposes and within the framework of the relevant task.

Transmitting data where the content is not related to work is not permitted.

Using the internet for private purposes is only permitted within the framework of the existing rules and regulations in the company.

The use of private software and data on the IT equipment provided by the company is prohibited.

A.1.2 The following rules apply to data security and the protection of personal data:

- In terms of classification, personal data that goes beyond business communication data is deemed to be at least confidential and requires technical encryption and strong authentication (e.g. a PKI certificate). Any deviations are to be agreed with the data privacy department at ALTEN.
- The erasure and/or disposal of employee data is be handled in accordance with Item A 1.3 below, in line with its classification.

A.1.3 The following rules apply to erasure or disposal of data:

- Strictly confidential paper documents are to be disposed of using a shredder with security level P-5 or higher.
- Confidential paper documents are to be shredded in accordance with security level P-4 or higher (data bins or shredder).
- Before being re-used or disposed of, data carriers must be wiped by completely erasing the information (e.g. irreversible formatting) or by suitable disposal (e.g. mechanical destruction).
- Where possible, data carriers should be wiped in line with the data erasure procedure BSI 2011 or at least Standard 5220.22-M of the Department of Defense.
- If the data carrier is an SSD hard drive or generally a flash drive, it is mandatory to use the Gutmann method.
- Data carriers that are no longer required are to be reliably erased by overwriting or by physically destroying them.
- The destruction of hard drives and other storage media is to be recorded and is to be carried out by a certified disposal company.
- Optical data carriers (CD, DVD, Blu-ray, etc.) and magnetic tapes must also be physically destroyed in order to ensure the reliable obliteration of the stored information.

A.1.4 Help desk: IT support: Tel. +49 9561 / 5533-560 – email: support@de.alten.com

A.1.5 ALTEN Information Security Team: Fax. +49 9561 / 5533-759 – email: informationssicherheit@de.alten.com

A.1.6 ALTEN Data Privacy DE: Fax. +49 9561 / 5533-725 – email: datenschutz@de.alten.com

ALTEN Data Privacy AT: Fax. +43 316 / 401485-27 – email: datenschutz@alten.at

A.1.7 Responsibility: The central contact for compliance with statutory obligations is the legal department at ALTEN (email: legal@de.alten.com)

A.1.8 In the Federal Republic of Germany, the current version of the German Data Protection Act - new (BDSG-neu) and the European General Data Protection Act (EU-DSGVO) as amended apply.

In the Republic of Austria, the current version of the Data Protection Act (DSG) and the European General Data Protection Act (EU-DSGVO) as amended apply.