# Guideline on Information Security and Data Protection for IT Service Providers
# juwi AG

Guideline

## Aim of the Guideline

The juwi Group has laid out its strategy with regard to the protection of corporate information in a superordinate “Guideline on Information Security”. This is intended to ensure compliance wiht the internal stipulations regarding information security and the statutory regulations.
For this reason, the Information Security Officer of juwi AG has formulated requirements and stipulations for cooperation with IT service providers (hereinafter referred to as “Contractors”) in this “Guideline on Information Security and Data Protection for IT Service Providers”. It shall apply to IT services of all kinds for all companies within the juwi Group (hereinafter referred to as the “Client”).

## Scope

This Security Guideline is binding for physical and logical access to IT systems, services, information, data and applications in networks of the juwi Group (hereinafter referred to as the “juwi network”). It shall also apply for access to buildings and rooms with IT or technical components.

In individual cases, it can be augmented with additional assignment-related or system-related security guidelines.

Within his company, and where subcontractors are deployed, within these too, the Contractor shall ensure the observance of this Security Guideline.

## Responsibilities

Responsibility for the issue and implementation of this guideline, as well as reporting, lies with the ISB and Data Protection.

## 1. Terms and Abbreviations

ISB = Information Security Officer
juwi network = IT systems, services, information, data and applications in networks of the juwi Group
Contractor = IT service provider himself, his staff and the sub-contractors deployed by him, as well as their employees
Client = A company of the juwi Group
BSI = German Federal Office for Information Security
DSGVO = GDPR
BDSG = German Federal Data Protection Act

## 2. General Terms and Conditions

Access to the buildings and rooms/offices of the juwi Group must always be requested through a contact partner in the juwi Group. In cases in which the Contractor is issued with an access card, this must be displayed at all times. The Contractor and/or his staff are prohibited from moving around premises of the juwi Group unaccompanied.

## 3. Technical Security Guideline

### 3.1. Physical access and logical access rights

Physical and logical accesss rights for the juwi network shall be granted as needed and, where necessary, restricted. The arrangement of physical access and logical access rights for the juwi network shall ensue through juwi IT Support and must be requested there by the Client.

When physical access/logical access to the juwi network has been set up for a Contractor, the following rules are to be observed:

a) Each employee of the Contractor must register using the user ID issued to him by juwi. The Client draws the Contractor's attention to the fact that physical and logical access to the juwi network is logged. The Contractor shall inform his staff and subcontractors of same. User IDs and passwords may not be passed on to others.
b) The Contractor is obliged to inform the Client without delay when physical /logical access to the juwi network is no longer required (e.g. completion of the contract, employee turnover, serving of notice or other terminaton of the contract).

### 3.2. Administration privileges

Where the Contractor requires administration privileges in order to execute the contract, this can be set up upon application of the Contractor to the Client. They are subject to the work instruction "Use of privileged accounts".

The setting up, alteration and deletion of administration privileges for systems within the juwi network shall ensue through juwi IT Support.

System administrators employed by juwi, plan, install, configure and update the IT infrastructure. Within the framework of their administrative duties and privileges, they ensure

a) correct installation,
b) trouble-free operation,
c) appropriate updating of the IT systems and applications and
d) observance of the objectives of information security (confidentiality, integrity, availability) in their area of responsibility.

The Contractor who has been issued with administration privileges must observe the following rules:

a) The administration privileges granted for the execution of the contract may be used exclusively for the intended purpose. Any passing on and/or transfer of the administration privileges personally assigned for execution of the contract and related user IDs and passwords is prohibited.
b) Should farther-reaching authorisation other than that necessary for the execution of the contract be set up for technical or organisational reasons, only such authorisation may be used as is absolutely necessary for execution of the contract.

c) Unauthorised physical and logical access to the Client's juwi network and access outside of the contract are prohibited.
d) The bypassing of security measures and encoders is prohibited.
e) In the execution of administrative duties, close attention must be paid to the strict ensuring of the confidentiality, availability and integrity of the juwi network.
f) Where, due to personnel-related, organisational or technical measures or changes, the requirements for the granting of administration privileges are no longer being met, either partially or in full, or where administration privileges are no longer required, the Contractor must notify the Client immediately.

## 3.3. Protection of the movement of information

Should, for the purpose of executing the contract, information be transferred to and/or processed on IT sysems of the Contractor – outside of the juwi network or integrated into same – and exchanged with the Client and/or companies of the juwi Group, the following security measures for the protection of the information and the juwi network are to be observed:

a) The Contractor must ensure that the latest version of a recognised secure anti-virus system with a regularly-updated virus signature databank is installed on the hardware (e.g. PCs, servers, gateways) used and provided by him, which offers protection against malware attacks (e.g. viruses, worms, Trojan horses) in particular via e-mail, web, mobile data carriers (e.g. USB flash drives) or other media by controlling the data access.
b) Where confidential information is exchanged between the juwi network and the network of the Contractor, the information is to be protected to a state-of-the-art standard and/or the transfer/transport must ensue via a secure connection/means of transport. For the exchange of strictly confidential information, content encryption (container, hardware encryption) and protected transmission/transport are mandatory.
c) The Contractor must ensure by means of a defined process that correctly-licenced software and regularly-updated security patches for the operating system software and applications are installed on the hardware used by him.

## 3.4. Connection to IT systems

In the case of a connection between IT systems of the Contractor's network and the juwi network, the following rules are to be observed:

a) When a connection is established to the juwi network, the Contractor must ensue that his own network does not facilitate uncontrolled logical access by third parties to the juwi network.
b) The Client assumes no responsibility for any damage to adjascent systems of the Contractor which may occur while the Contractor is connected to the juwi network.

## 3.5. Physical and logical access

Physical and logical access must be requested by the Client from juwi IT Support.

Prior to the setting up of physical and logical access rights (see 3.2), the Contractor was awarded the contract and, in this context; informed of this Security Guideline as well of the use of privileged accounts. Where applicable, the Client shall inform the Contractor's employees of this Security Guideline and issue a separate "Commitment to data secrecy and information security" for signing. Physical and logical access for external employees shall be limited to the intended duration of the contract, at a maximum, however, to twelve (12) months.

The activities shall be logged and, where appropriate, analysed. The Contractor shall inform his staff and subcontractors of same.

### 3.6. Use of wireless components

The use of wireless components belonging to the Contractor in premises of the juwi Group may not negatively impact on the existing equipment and no connection to the juwi network may be established.

### 3.7. Secure system and applications operation

If IT systems, applications and IT infrastructure are operated or administered by the Contractor on the instructions of the Client in premises of the juwi Group or the Contractor (application service provider), the following rules shall apply:

a) The operation must comply with the information protection requirements in order to be recognised as trustworthy. In particular,
   I. The statutory stipulations must be observed
   II. The general BSI security standards and/or ISO 27001 must be observed,
   III. The best available technology with regard to the secure collection, processing, dissemination, storage and safekeeping, transmissions and deletion/disposal of information requiring protection and
   IV. The requirements in terms of communication and escalation processes with regard to events of information protection relevance are to be observed.

b) The Contractor must take appropriate precautionary measures to protect the hardware components from physical damage and prevent use by unauthorised users.

c) The Contractor must guarantee the security of the operating environment and implement physical and logical access controls.

d) Where the contract involves the collection, use or processing of personal data within the meaning of the General Data Protection Regulation and the German Federal Data Protection Act, the Contractor must take all the measures dictated by statutory stipulations to protect the data.

### 3.8. Software development and integration

Where the Contractor renders services or software development and/or integration, the project-specific security requirements agreed separately between Client and Contractor are to be implemented, taking this Security Guidline into account.

## 4. General Obligations

### 4.1. Use of Client Information

The Contractor is obliged to use the physical/logical access rights to the juwi networks granted by the Client exclusively in the context of the duties to be performed under the contract.

All information not already in the public domain acquired through the contract, as well as copies, records and work results compiled in connection with the contract, are the property of the Client and are to be surrendered or returned to same upon termination of the contract.

The Contractor is obliged to treat all information on the Client and companies of the juwi Group, their business and operating matters and all work results which come to his notice in the context of the execution of the contract

confidentially and prevent their being disclosed to unauthorised persons and non-contractual use, reproduction or transmission. These obligations shall continue to apply beyond the termination of the contractual relationship.

The Contractor is not permitted to acquire business or operating information of any kind regarding the Client and/or his customer, supplier or staff which has not been made public by the juwi Group or to use or copy same for his own purposes or to make copies or records of any kind which are not necessary for the execution of the contract. Information, copies, records or work results of this kind may not be passed on to third parties or disclosed to third parties.

Confidential information may only be passed on to the subcontractors who have been approved by the Client and bound to observance of the above Security Guideline. Proof of same is to be provided by the Contractor at the Client's request.

## 4.2. Data protection

The Contractor guarantees that he complies with all valid data protection legislation, specifically the EU General Data Protection Regulations and the 2018 German Federal Data Protection Act and that he has obtained all the permits relating to the handling and management of personal data necessary under current legislation. The Contractor shall indemnify the Client from all costs, claims, liabilities and demands arising for the Client with regard to an infringement of this guarantee.

The Contractor hereby declares that he has received and read the Client's "**Information on data processing for customers, suppliers and other data subjects"**. For the event that the data subject is not also the Contractor, the Contractor hereby undertakes to pass this "Information on data processing for customers, suppliers and other data subjects" on to the data subjects who will have contact with the Client in the context of this contractual relationship on the intitiative of the Contractor.

Where, in the context of this contractual relationship, the Contractor is acting as a processor within the meaning of Art. 28 GDPR, the Contractor and Client will first conclude a processing agreement in compliance with the statutory stipulations. The Contractor and Client shall be jointly and severally liable for compensation for losses suffered by any person due to inadmissable or incorrect data processing in the context of the contractual relationship. The Contractor shall bear the burden of proving that the losses are not the result of a circumstance for which he is responsible where the relevant data was processed under this agreement. Until such time as this proof has been presented, the Contractor shall indemnify the Client, at first request, from all claims, demands, liability of third parties or vis-a-vis third parties and for costs charged against the Client in the context of the processing. The Contractor shall be liable to the Client for damage culpably caused by the Contractor. Point 4.2 Data Protection shall not apply provided the damage results from the correct implementation of commissioned services or actions carried out on the instructions of the Client.

The Contractor undertakes to deploy only such staff as have been bound to data secrecy pursuant to Section 5 BDSG (old) or to the observance of confidentiality within the meaning of the DSGVO and where this obligation continues to apply for the period following termination of their employment with the Contractor.

Regardless of the statuturory stipulations, any passing on of the Client's personal data to third parties by the Contractor requires the prior written approval of the Client. The Contractor undertakes only to commission subcontractors with the processing of the Client's personal data when these have previously been bound in writing to the observance of the obligations pursuant to Point 4.2. Data Protection in the same manner as the Contractor.

### 4.3. Personal suitability and professional qualifications of the employee

The Contractor is obliged to deploy only empoyees at the Clients who are personally suitable and professionally qualified. The Contractor is to assess the employee prior to the beginning of the employment.

The Contractor must ensue that the employee whose personal and/or professional suitability cannot be adequately assessed shall neither have physical access to the site or the building nor logical access to the Client's juwi network.

At the request of the Client, the Contractor shall submit suitable documents for the assessment of the personal and professional suitability to the Client.

Item 4.3 shall apply accordingly for staff of the subcontractor.

## 5. Monitoring of the Observance of the Security Guideline, Notification Requirement and Blocking of Physical and Logical Access

The Client shall also have the right to monitor the observance of this Security Guideline at the Contractor's site. Furthermore, the Contractor must permit the Client to carry out inspections at his subcontractor's sites.

The Contractor shall permit the Client access, in particular following prior notification and within normal business hours, to all relevant operating sites and shall support him with all necessary activities. Furthermore, he shall permit inspection of the documentation of operational relevance for the juwi network.

Furthermore, the Client reserves the right to modify the type of physical/logical access of the Contractor to the juwi network in order to guarantee the security of the juwi network.

The Contractor is obliged to comply with the security regulations and laws relevant for him, and to ensure tamper-proof documentation of all relevant errors, irregularities or security incidents as well as initiated measures to eliminate same in the context of the juwi network, and report same immediately to the Client.