Stadtwerke München

Information security

Regulations on the use of IT systems for external parties

1. Objective

You received a business order from SWM for which you will use SWM IT systems. It is necessary to comply with certain regulations in order to ensure the level of information security at SWM when using external services. This document contains the most important rules of procedure for users to ensure that the company's own data and information resources are protected. Compliance with the following technical and organisational security measures is a basic prerequisite for being allowed to use SWM's IT systems.

2. Fundamental rules of information security

2.1. **SWM's IT systems and applications are to be used exclusively for the purposes of the tasks and activities assigned to them.** It is prohibited in the SWM communication and process network, to use IT systems that do not belong to SWM. You must obtain authorisation from the responsible system operator or network operator via the commissioning department should this be necessary for order processing.

2.2. SWM’s information resources must be protected against malware.

a) However, you must check these for malware before installation and obtain approval from the system operator or the person responsible for the system should your business order include the commissioning of hardware and software.
b) It is prohibited to use and/or distribute malware, programmes or hardware in SWM's communication and process networks that can change or manipulate information resources. In the course of security audits and penetration tests
the use of software to detect vulnerabilities must be coordinated with the person responsible for information security.

2.3. Personal and company-related data may not be passed on to third parties without authorisation or used for your own purposes. You may only use this data for the fulfilment of your order.

2.4. Protocol and evaluation procedures for systems and applications can be used to increase security.

2.5. You must notify the client immediately of any incidents that may have an impact on information security (such as signs of a virus attack).

3. SWM user ID

3.1. Access to information resources, IT systems, and applications is via multi-factor authentication (MFA). You will receive a personal user ID and additionally require a hardware or software-based multi-factor.

The software factor (token) is installed via an app on a mobile device of the contractor. Access information (user ID, passwords/PIN) may not be shared with or used by third parties.

3.2. The token issued for dynamic password generation (one-time password) may be passed on to authorised employees authorised by SWM as part of a maintenance and standby order.

3.3. It is prohibited to find out and try out user IDs of other IT users.

4. Communication

4.1. You may only use Internet and e-mail services for the fulfilment of the commissioned operation. The services are subject to centralised and automated protection procedures (virus protection, spam checks, blocking and filtering of e-mails, restricted download authorisations and website revocation lists).

4.2. Connections from the internal SWM network to external networks (e.g. to the Internet) may only be made via dedicated firewall computers. Modems or wireless connections to third-party networks may not be used in combination with an active SWM network connection.

4.3. It is forbidden to explore the network topology or the configuration of SWM's IT systems and applications.

4.4. Integration of third-party computer systems

Should third-party computer systems require a connection to SWM's network or domain infrastructure due to the business contract, the following conditions must be met:

- Current and active virus scanner (engine and pattern),
- Current patch level for the operating system.

If you have any questions, please contact your specialist contact person at SWM.

5. Remote maintenance and remote access to SWM’s IT infrastructure

Remote access and network connections to SWM's IT infrastructure are carried out in accordance with stipulated regulations:

5.1. Remote maintenance shall be carried out exclusively within the framework of the agreements made and in accordance with SWM's instructions.

5.2. The Contractor shall inform SWM in writing before the start of the remote maintenance which employees it will deploy for this purpose.

5.3. Data transmissions must be encrypted in accordance with the state of the art.

5.4. The beginning of each remote maintenance must be announced in order to give SWM's authorised representatives the opportunity to follow the remote maintenance measures.

5.5. The connection establishment must be carried out by the SWM or initiated by the local SWM systems so that maintenance work can be carried out by authorized persons solely and with the knowledge and consent of the SWM.

5.6. When data (including programmes, updates, patches) are stored and/or started on SWM's systems, suitable means must be used to ensure that they are free of malware.

5.7. SWM has the right to interrupt remote maintenance, in particular if unauthorised access is made to files or to hardware and software components that have not been previously consented to.

5.8. Access shall be logged by SWM's system operators.

Notwithstanding the above provisions, an external party that administers or maintains systems in the SWM infrastructure on behalf of SWM may be granted access that does not have to be initiated by SWM. This requires that one of the following points applies:

- Maintaining trouble-free operations
- Ensuring prompt fault clearance
- Access to test and development systems

This does not affect the obligation to provide documentation and to notify SWM at the start of remote access.

6. Access to SWM Premises

6.1. Conduct on SWM Premises

The following rules of conduct must be observed:

- Carry an SWM visitor badge or an identification document of the contracted company at all times.

- SWM PCs and laptops must not be used without prior authorization.
- Information and media, regardless of format, must not be removed or copied.
- Photo, video, and audio recordings are prohibited.

6.2. Handling of Access Media

When handling access media (e.g. keys, ID-cards), the following rules must be observed:

- Access media must never be passed on to other persons and must be kept secure at all times.
- The loss of access media constitutes a security-relevant incident and must be reported immediately by the employee.

7. Verification and control

SWM's responsible person for information security may carry out unannounced checks to verify compliance with the requirements.

8. Acknowledgement of the regulations on information security at SWM

I hereby confirm that I have received and taken note of the document:

“REGULATIONS ON THE USE OF IT SYSTEMS FOR EXTERNAL PARTIES“

Company: ……

Surname: ……

Name: ……

Date: …… **Signature: ……**