IMF
INGENIEURGESELLSCHAFT
MEINHARDT FULST

Policy

INFORMATION SECURITY FOR SUPPLIERS AND PARTNERS

Ingenieurgesellschaft Meinhardt Fulst GmbH
Kaiserstraße 18
38690 Goslar

Classification: PUBLIC

Version 1.1
28. July 2025

TABLE OF CONTENTS

1 Purpose, scope, and users

This document is binding at the IMF in all locations, for all suppliers, service providers, and contractors (hereinafter referred to as "contractors") and for all types of information, regardless of their form (paper or electronic documents, applications and databases, personal knowledge, etc.).

For reasons of better comprehensibility, the generic masculine form is used in this document. Female and other gender identities are expressly mentioned where necessary for the meaning.

In the event of any discrepancies between the different language versions of this contract, the German version shall prevail.

The purpose of this document is to establish rules for the handling of information and the use of information technology, which the Contractor must comply with.

The rules serve to protect the confidentiality, integrity, and availability of information as well as the rights and interests of IMF as the client and of all natural and legal persons who enter into a business relationship with IMF and/or perform activities for IMF. The rules set out in this document supplement or specify the confidentiality obligations and/or contracts for order processing agreed between IMF and the supplier and its employees.

2 Basic rules on confidentiality and the protection of personal data

IMF works exclusively with ISMS-relevant suppliers and partners who have committed themselves to maintaining the confidentiality of data, information, and trade secrets within the framework of the corresponding declaration of commitment or another confidentiality agreement (NDA).

If the contractor processes personal data on behalf of IMF, an additional data processing agreement (DPA) must be concluded before the contracted work is commenced.

Data and information about IMF or data and information that becomes known in the course of performing tasks may not be passed on to third parties or published, in particular on social networks (e.g., Facebook, Google+, LinkedIn, XING, etc.) or elsewhere, in particular on the Internet (e.g., Twitter, YouTube, etc.). Exceptions shall only be made if the data is generally accessible, the contractual relationship specifically provides for such disclosure or publication of data, or IMF has given its express consent.

3 Regulations on the handling of information and information-processing facilities

3.1 General

If, in connection with the contractual performance of tasks, it is necessary for the Contractor to process or store data or information outside the IMF's systems, the IMF must be informed of this in writing by the Supplier before processing or storage begins. The IMF must give its consent to this, unless this is already clear from the contract.

The removal or removal by IMF of hardware and software provided for the performance of tasks from IMF locations is prohibited without the express permission of IMF. Unauthorized extensions to the hardware provided by IMF and the connection of peripheral devices and external storage devices are also prohibited without the express permission of IMF. Modifications or extensions may only be carried out by the system administrators of IMF.

If the Contractor wishes to use the IMF's email system, network, or IT systems to fulfill its contractual obligations, it is obliged to obtain express permission before using the services or connecting any systems. Furthermore, the Contractor must regularly inform itself of the current internal rules for handling these systems and media from the designated IMF contact person and comply with these rules. For example, the disclosure of configuration and access data, as well as identification means, without the written consent of IMF is not permitted and constitutes a reportable incident. IMF reserves the right to access all systems, data, and information provided without prior notice.

The use of IMF systems and media for private purposes is expressly prohibited. The use of private devices belonging to employees or vicarious agents of the Contractor for the performance of the services contractually agreed with IMF is also expressly prohibited, even if this is regulated and permitted internally by the Contractor through appropriate guidelines.

When processing IMF information, the Contractor must ensure that the protection objectives of availability, confidentiality, and integrity are met in accordance with the current state of the art. The Contractor is required to take appropriate measures, such as protection against malicious code, access controls, clear desk and clear screen policies, backup of information, employee awareness and protection, etc.

3.2 Classification of information

The IMF classifies information according to the level of confidentiality required, taking into account the additional protection objectives of integrity and availability. Four different information classifications are used for this purpose:

- PUBLIC – the information is public
- INTERNAL – the information is available to all employees and third parties selected by IMF or contractors
- CONFIDENTIAL – the information is only accessible to a specific group of employees and third parties authorized by IMF
- TOP SECRET – the information is only accessible to individual employees; if this information is exchanged with external parties for justified reasons, personal delivery must be ensured

3.3 Labeling of classified information

In order to inform about the need to protect information from unauthorized access, information classified as "CONFIDENTIAL" and "TOP SECRET" should be labeled as such wherever possible. This can be done, for example, by labeling file folders, project folders, notes in email subject lines, in file names, in document headers or footers, in letters, e.g., by means of an inner envelope with the addition "confidential – for the attention of ..." etc.

The Contractor is responsible for informing its employees and vicarious agents accordingly and for initiating appropriate measures to protect the information.

3.4 Handling of classified information

In particular, the processing of information classified and labeled as "CONFIDENTIAL" or "TOP SECRET" within the scope of the cooperation is subject to special protection requirements. The Contractor, its employees, and its vicarious agents may only pass on information in accordance with the classification within the approved or commissioned scope and in accordance with the "need-to-know principle." In addition, the following measures must be implemented to protect the information:

- When storing information marked accordingly, the Contractor must ensure strict access control and appropriate client separation.
- Processing, in particular the storage of information classified as "CONFIDENTIAL" or "TOP SECRET" in countries outside the EU, for example in the context of using a cloud service provider, is only permitted with the express permission of the IMF.
- If the Contractor uses cloud services that are not exclusively under its own control for the necessary storage and processing, information classified as "CONFIDENTIAL" or "TOP SECRET" by the IMF must also be protected against unauthorized access by means of encryption and multi-factor authentication (MFA). Any backups outsourced to cloud services must be encrypted before transfer.
- Information classified as "CONFIDENTIAL" or "TOP SECRET" must not be stored unencrypted on mobile data carriers and end devices (notebooks, smartphones, USB data carriers, etc.).
- When transporting or transmitting information classified as "CONFIDENTIAL" or "TOP SECRET" via public networks, it must always be encrypted using state-of-the-art encryption. This applies in particular to communication by email.
- Upon termination or amendment of the contractual relationship and upon expiry of regulatory deadlines, the relevant information must be returned to IMF or deleted in accordance with IMF's instructions. In the event of a statutory archiving or retention obligation on the part of the Contractor that extends beyond the duration of the contractual cooperation, the level of protection of the classified information must be maintained until it is deleted or destroyed.
- When destroying or deleting data/information and information carriers (including electronic data carriers and paper files), these must be disposed of in accordance with security level 3 for information classified as "CONFIDENTIAL" and security level 4 for information classified as "TOP SECRET" in accordance with DIN 66399.

4 Reporting security vulnerabilities and incidents

Definition: Security vulnerability – no incident has occurred yet, but an event related to a system, process, or organization could result in an incident in the near or distant future . A risk has not yet materialized, which means that a threat has not yet exploited the vulnerability.

Examples of security vulnerabilities include:

- Recurring unimplemented technical and organizational measures

Definition: Incident - an incident that could cause damage through the loss of confidentiality or integrity and, as a result, authenticity of information, or that could cause an interruption in the availability of information and/or processes. Examples of incidents are:

- Hacker attacks
- Malicious code or ransomware attacks
- Leakage of confidential information or authentication data, as well as data breaches
- Loss of work equipment, such as IT devices used to process or store IMF data or provided as means of identification (e.g., keys, ID cards, or cryptographic tokens)
- Interruption of the availability of IT systems or cloud services with an impact on the value chain

The contractor, its employees, and agents must report any incidents to the contract managers and management at the IMF if the information or personal data of the IMF is affected.

In addition, the Contractor, its employees, and vicarious agents must report any identified security vulnerabilities in systems or processes that serve to protect IMF information classified as "CONFIDENTIAL" or "TOP SECRET" to the contract manager designated by IMF and to the management.

Incidents and security vulnerabilities must be reported in writing (e.g., by email), classified as "CONFIDENTIAL" at a minimum, and must include the following information:

- Type (brief description) of the incident or vulnerability
- Type of information affected (classification, personal reference, number/scope of data quantities)
- Time of occurrence and/or first knowledge
- Initial measures taken and/or planned measures for handling
- Responsible contact person and their contact information

5 Awareness and reviews

The Contractor must ensure compliance with the information security regulations contained in this document within its area of responsibility. In this context, the Contractor must ensure that all relevant employees and vicarious agents are sufficiently sensitized, familiarized with the regulations, and comply with them.

The IMF has the right, in consultation with the Contractor, to carry out checks on compliance with these security guidelines to the extent necessary or to have them carried out by an auditor to be appointed in each individual case. The Contractor shall provide the IMF with all information necessary to fulfill its internal control function ( ). In the event of a change to the contract or termination of the contract, the Contractor shall, upon request, inform the IMF which confidential information has been returned or destroyed and which has been retained. The notification that certain documents or information have been retained must be justified.

Within the scope of the cooperation, the Contractor is required to regularly and independently inform itself about the current regulations and guidelines at the IMF and to comply with them.

6 Contact

6.1 Information Security Officer (ISMS Committee)

To report information security incidents and vulnerabilities, please contact our ISMS Committee, tel. +49 (0) 5324/7799-0, email: ISMS_Ausschuss@i-mf.de

6.2 Data Protection Officer (DPO)

If you have any questions about data protection, please contact our data protection officer, the Kämmer Consulting team. Tel +49 (0) 531/702249-0, email: dsb-team@kaemmer-consulting.de.