Preamble

NMA operates an Information Security Management System (ISMS) with the aim of ensuring the confidentiality, availability, and integrity of processed data or relevant systems. Suppliers also contribute significantly to information security through their services and products, which is why this document defines corresponding regulations.

1. General

The supplier undertakes to effectively secure all information and data collected or processed for NMA against unauthorized access, alteration, destruction, or loss, unauthorized processing, and other misuse, always according to the current state of the art. When accessing (including remote access) NMA's information processing systems, the supplier must comply with the applicable regulations and guidelines for information security provided by NMA upon request.

2. Communication

Upon request, the supplier provides NMA with the name and contact details of the designated information security contact person. Any change of the contact person must be promptly notified. The parties inform each other immediately if they detect errors or irregularities in processes, security checks, or examination of the results of the assignment.

3. Handling of Information

Provided information must be securely stored and returned to the owner upon request, with the supplier not retaining any copies, duplicates, or other documentation of the provided information in this case. Information and programs may only be transferred to or from NMA's information processing systems within the scope of the agreed activities and with NMA's approval. Access must only be from systems whose security level complies with NMA's information security requirements. The supplier is obligated to treat all knowledge gained about NMA's information security measures confidentially, even beyond the end of the contractual relationship. The supplier must examine all data transfers (e.g., via email or data transfer, data carriers) used in the provision of services for malware (e.g., Trojans, viruses, spyware, etc.) using current testing and analysis methods before provision or use, ensuring that they are free of malware. If malware is detected, the data transfer may not take place. If the supplier detects malware at NMA, they will promptly inform NMA about it.

4. Access Rights

NMA will only provide the supplier with the access rights necessary to perform the agreed activities, regularly verify their currency, and make corrections if necessary. The supplier may only use the access rights granted to them to the extent necessary for performing the activities. NMA has the right to interrupt the supplier's access to NMA's information processing systems, especially if there is suspicion of unauthorized access to information and resources. Necessary data transfers for access purposes must be sufficiently encrypted; exceptions must be adequately justified.

5. Information Security Review

NMA is entitled to monitor or have monitored the compliance with the provisions of this agreement to the necessary extent. After consultation, the supplier grants unhindered access to information processing systems, programs, and information related to the performance of the activities. The supplier must

provide NMA with all information necessary to fulfill the monitoring function. NMA is entitled to log and evaluate all actions of the supplier within their information processing systems.

6. Employees/Subcontractors

The supplier informs their employees, subcontractors, or freelance workers deployed at NMA about relevant information security topics. The supplier may only use subcontractors or freelance workers with NMA's written consent.

7. Termination of Contract

Upon termination of the contract, access permissions of the relevant personnel of the supplier to NMA's systems and premises cease. The supplier simultaneously returns any equipment, IDs, and other items provided for authentication (e.g. tokens, smart cards) without prompting.