MM Security Requirements for Suppliers of the MM Group

Security of supply and safe services are key corporate strategy elements of MM Group (Mayr-Melnhof Karton Aktiengesellschaft and its affiliated companies; those affiliated companies - hereinafter referred to as "MM" or “we”- are available at www.mm.group/en/legal-entities/). It is important to us to protect data, systems, and applications with security measures in accordance with leading industry standards, as is expected of one of the leading Austrian groups in the manufacturing sectors. Managing Supplier relationships with regard to security is an important part of our internal risk management, a common practice under international standards (e.g., ISO 27000 series, NIST Cybersecurity Framework).

MM´s Bidder, Processor, Contractor or Contracting Party (hereinafter referred to as "Supplier) represents and warrants that it has fulfilled all necessary due diligence obligations, is familiar with and acknowledges these Security Requirements, and agrees to comply with them when:

- accessing MM facilities, networks and/or information systems; or
- accessing, processing, or storing MM information/data; or
- providing IT infrastructure services and/or standard software, or developing software.

Any reference herein to "Customer" is a reference not only to MM data (or systems, services, etc.), but also to the data of MM Customers and Partners. Additional security requirements may be specified in individual agreements (e.g.: SLA, requirements catalog). These Security Requirements supplement the provisions on confidentiality and security in the General Terms and Conditions of Purchase of the MM Group. Individual agreements between Supplier and Customer which replace or supplement this Agreement in whole or in part shall take precedence over this Agreement. However, General Terms etc. by the Supplier shall not take precedence over this Agreement.

Contents

1 Governance

1.1 Guidelines

The Supplier operates an information security management system that is subject to a continuous improvement process based on recognized standards.

Information security policies, procedures, roles, responsibilities, and accountabilities are stipulated in accordance with the Supplier's business requirements, relevant laws, regulations, and common security standards. Information security policies are approved by management, published, and communicated to employees and relevant external parties.

The Supplier agrees to verify its compliance with the established information security policies and standards, and all other information security requirements, on a regular basis.

1.2 Risk Management

The Supplier has implemented an information security risk management program. The Supplier ensures that risks that have a direct or indirect effect on the Customer's services and/or data are assessed and that risk mitigation measures are taken and documented. Risks that directly or indirectly affect the Customer must be reported on request.

1.3 Information Classification

As not all information has the same sensitivity, information must be classified into degrees of confidentiality. The confidentiality classes can be seen as a measure of the impact any misuse of information can have. If the Customer provides the Supplier with information, it shall be classified as follows. Classification is into 4 classes (public, internal, confidential, and strictly confidential), which regulate how the respective information is to be handled.

- public: Information that is publicly available and where its publication has no detrimental effect on the activities, assets or image of the Customer
- internal: Information that is used within the Customer by internal or authorized personnel, which if communicated externally, could have a minor detrimental effect on the activities, assets or image of the Customer
- confidential: Information that is known only to a limited number of individuals and if revealed, could be detrimental to the commercial activities, assets or image of the Customer; sensitive personal data treated as confidential Information
- strictly confidential: business-critical Information that could seriously damage the activities, assets or image of the Customer if released inappropriately; prototypes, among other things, prototypes, recipes, production processes are treated as strictly confidential

1.4 Contractual Agreements

The Supplier agrees to include responsibility for information security in the contractual agreements with its employees and contractors.

1.5 Background Checks

Background checks of candidates for employment are conducted in accordance with applicable laws and regulations. The extent of such checks must be proportionate to the risk associated with the candidate's role. Example: In Austria, criminal record certificate, or similar verification mechanisms in other countries (criminal record extract).

1.6 Awareness Program

All of the Supplier's employees and, where relevant, contractors, undergo awareness-raising and training measures appropriate to their role. In addition, employees will also be informed of updates to the Supplier's policies and procedures. All employees must have the skills required for their roles and responsibilities.

2 Change Management

2.1 Asset lifecycle

The Supplier ensures information security to be an integral part of information systems throughout their lifecycle (acquisition to decommissioning and disposal of equipment and systems). The Supplier ensures that the provided components and their operating systems, middleware (e.g., Java) and applications are supported and receive the latest security updates. The Supplier provides regular security updates in good time throughout the term of the contract.

After termination of the contractual relationship the Supplier ensures the returning to the Customer of components (e.g., devices, media) provided to it.

2.2 Software Change Management

The Supplier has implemented formal policies regarding change management and secure software development lifecycle that also define security-related checks. Cybersecurity reviews of new system designs or system changes, as well as security testing prior to their implementation must be part of the processes. Prior to being released for production, changes are appropriately requested, authorized, tested, and approved.

2.3 Secure Software Development Lifecycle

The Supplier includes information security aspects in its product documentation. Such documentation must include instructions for the configuration of the service and/or the environment to ensure secure

operation. The software developed must be tested in a controlled environment in order to detect flaws before it is made available to the Customer.

The Supplier ensures that the software development lifecycle contains appropriate security measures (Secure Software Development Lifecycle). These includes, but are not limited to:

- employing internationally recognized secure software development methods (including agile processes such as Scrum, Kanban, etc.) as integral elements of the secure software development process;
- secure coding guidelines based on international standards;
- ensuring the integrity of the source code;
- regular secure code reviews (static and dynamic application security tests);
- vulnerability scans that include third-party code and open-source components (e.g., libraries) in use;
- security and penetration tests performed by an independent third party;
- appropriate training for internal and external software developers.
- Detected and known vulnerabilities are eliminated before release for production.

3 Outsourcing

3.1 Sub-Outsourcing

The Supplier has clear contractual agreements with all subcontractors of services in order to establish their responsibility for the security of the Customer data they process/store/transmit on behalf of the Customer. The Supplier ensures that the security measures implemented by the subcontractors match or exceed the level specified herein and in the main contract. The Supplier, as part of the Supplier management process, verifies the effectiveness of these measures.

4 Secure System Operation

4.1 Identity and Access Management

The Supplier has implemented access controls to verify identities and restrict access to authorized users. Access rights are based on the principle of minimum access and the function-based necessity of access. In addition, the principle of "segregation of duties" is respected.

The Supplier has implemented best-practice authentication mechanisms to protect system access that include, but are not limited to:

- password policy (minimum 14 characters, complexity, no reuse);
- unique user identification (avoid generic and joint users);
- secure storage/management/transmission of login credentials.

The Supplier ensures the protection of accounts that can be accessed via the Internet by strong authentication mechanisms, at least multi-factor authentication.

The Supplier has implemented strict privileged account controls (e.g., accounts for system administrators) through strong authentication requirements (e.g., multi-factor authentication), restriction to a minimum and closely monitored usage.

The Supplier reviews employee access rights at regular intervals (at least once a year) and modifies (i.e., restricts/revokes) them if need be. The Supplier informs the Customer of the end/termination of employment of employees with access rights. All means of access (e.g., keys, access cards, remote access tokens) are to be returned to the Customer without delay.

4.2 Patch Management

The Supplier performs regular system analyses (operating systems, applications, network components) for known vulnerabilities. Patches are applied in a consistent and standardized manner, prioritized according to their criticality. If the root of vulnerabilities cannot be remedied within a reasonable period of time, alternative risk mitigation measures must be taken until remediation has been achieved. The Supplier has implemented an emergency change process.

4.3 Network Security

The Supplier has implemented and maintains network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS), or other security controls that enable detection, continuous monitoring, and restriction of network traffic to limit the impact of attacks. Stricter measures must be in place for systems posing higher risk (e.g., systems for access from external networks).

The Supplier ensures the implementation of a formal remote access policy.

The Supplier's remote access to the Customer's networks and systems is subject to the terms and conditions and security specifications communicated to that effect by the Customer and contingent upon the conclusion of a separate remote access agreement.

The Supplier ensures industry-standard segregation and segmentation of environments if:

- environments are shared with other Customers; and/or
- the Supplier sets up test, quality and production environments.

4.4 Encryption

The Supplier ensures adequate protection of the confidentiality of the data. The Supplier must also consider specific measures for data in transit and in volatile and non-volatile memory, such as the use of encryption technologies in combination with an appropriate key management architecture. Encryption is in

accord with leading standards and guidelines or equivalents (e.g., National Institute of Standards and Technology - NIST).

The Supplier protects mobile devices and external electronic media (e.g., USB flash drives, portable hard disks, tapes) from unauthorized access through appropriate physical and logical security measures. The encryption of data stored on such devices must be ensured.

4.5 Protection from Malware

The Supplier uses adequate and continuously updated blocking tools to protect servers and end devices from malware. The software must be able to detect if the antivirus/malware software on devices has been disabled or is not updated regularly.

4.6 Security Review & Monitoring

The Supplier has implemented appropriate security measures (with regard to cyber threats in particular) for data, applications and systems. The Supplier regularly evaluates the effectiveness of security measures with regard to known cyber threats and fraud as well as corresponding models (e.g., based on current threat catalogs published by the National Institute of Standards and Technology [NIST] and Federal Office for Information Security [BSI].).

The Supplier plans and conducts vulnerability assessments and penetration tests at regular intervals for all systems used to provide Customer services. On these systems, penetration tests must be performed:

- at least once a year;
- whenever there is a major release/update of applications/software/ information services;
- only by sufficiently knowledgeable, skilled, and experienced testers who were not involved in the security measures development.

Any vulnerabilities detected and the results obtained must be managed in an appropriate manner: analysis, classification, and remediation. Remedial actions must be implemented in accordance with criticality near to the time of detection. Upon request, the Supplier provides summary vulnerability assessment and/or penetration test result reports.

The Supplier ensures that security issues reported by the Customer are remedied within a reasonable period.

The Customer reserves the right to demand written proof of safety measures in accordance with Section 11 (1) (2) in conjunction with Annex 1 NISV. Evidence based on the following standards will be accepted for this purpose:

- ÖISHB: Cooperation with external parties, evaluation of certifications, supplier relations
- ISO/IEC 27001: Information security in supplier relationships

- IEC 62443 2-1: Supply chain security
- CIS CSC v8.0: Service provider management
- KSÖ Cyber Risk Rating: Requirements for A or B Rating

The Customer reserves the right to conduct security assessments and reviews in order to verify compliance with the requirements set forth herein. The Customer agrees to notify the Supplier in advance and ensures the audit is conducted during regular business hours with minimal disruption of the Supplier's business. Upon request, the Supplier confirms in writing its compliance with the requirements set forth herein and answers in writing any questions the Customer may ask the Supplier regarding its security procedures.

4.7 System Hardening

The Supplier configures and deploys its IT resources (e.g. databases, applications, operating systems, network devices) using a secure baseline (hardening). The secure baseline is in compliance with best practices (e.g., CIS standards) or equivalent standards. The configurations for the IT assets are regularly reviewed and updated.

5 Operation

5.1 Data Management

The Supplier ensures that measures are taken against data loss and leakage.

The Supplier must neither replicate Customer production data nor use them in non-production environments. Any use of Customer data in non-production environments is contingent upon the Customer's explicit and documented consent.

The Supplier ensures that, after termination of the contractual relationship, upon request information (physical, digital) is securely deleted or information carriers are returned.

5.2 Backup & Recovery

The Supplier ensures the existence of backup and data retention concepts for each relevant platform/component it is responsible for. Retention periods are checked and backups as well as recovery tests are performed. The backup concepts and recovery procedures are of a nature that ensures the agreed availability levels.

5.3 Logging & Monitoring

The Supplier has taken appropriate measures to ensure transparency and traceability of all operations carried out. Logs must be sufficiently detailed in order to assist in the identification of the source of a (security) issue and to enable a sequence of events to be recreated. Logs must be made available to the Customer if the Customer has justified reasons. Logs must record access attempts, information about

system and network security events, alerts, failures, and errors. Log file integrity must be guaranteed. Log file access must be restricted.

5.4 Incident Management & Reporting

The Supplier must have implemented documented information security incident procedures enabling the effective and orderly management of security incidents. The procedures must cover the reporting, analysis, monitoring, resolution, and documentation of security incidents, as well as response and recovery processes following a security incident.

The Supplier agrees to notify the Customer immediately upon becoming aware of any incident directly or indirectly related to the Customer's services and data by email to supplier-incident@mm.group, and to provide any information known to it to assist the Customer in fulfilling its obligations. The Supplier provides such information step by step as it becomes available. After verification of a security incident related to the Customer's services or data, the Supplier:

i. agrees to notify in addition the Customer's business units in writing;
ii. ensures that such notification contains at least the following information; if initially not all information is available, the Supplier should provide details - in the event of time-critical cases or imminent danger as soon as available - in a series of notifications:

- Contact information on the person at the Supplier responsible for the incident - What occurred?
- How did it occur?
- Why did it occur?
- Affected components/systems/assets
- Affected Customer services/data
- Date and time of occurrence of the incident
- Date and time of discovery of the incident
- Impact on the business / impact on Customer services/data
- Incident resolution
- Measures taken to resolve the incident
- Measures planned to resolve the incident

iii. makes every reasonable effort to detect and prevent such incidents;
iv. informs the Customer on an ongoing basis of the measures taken/planned to be taken by the Supplier;
v. obtains the Customer's prior written consent under applicable law in connection with any notification or public information relating to such breach; and
vi. coordinates all further activities with the Customer.
vii. This reporting requirement also applies to subcontractors.

6 Physical Security

6.1 Physical Access

The Supplier's premises have been categorized into different protection zones corresponding to the security measures and access rights in accordance with the relevant security requirements.

Physical access to IT systems, such as servers, is further restricted by special protection zones to which only authorized personnel has access.

7 Business Continuity Management

7.1 BCM

The Supplier has implemented current and continuously maintained disaster recovery and business continuity plans. Disaster recovery plans and business continuity plans must be designed to prevent, to the largest possible extent, any negative impacts from unplanned interruptions and to allow the Supplier, also in case of interruptions, to continue operating and providing services in accordance with its contract with the Customer. Upon request, the Supplier provides the Customer with written summaries of its disaster recovery and business continuity plans.

At least once a year, the Supplier conducts appropriate tests of its own business continuity and disaster recovery plans. Service-relevant test results are made available to the Customer upon request, but at least after such tests have been performed.

The Supplier has ensured that the scope of the business continuity and disaster recovery plans covers all locations, employees, and information systems used to provide services to the Customer.