TRUMPF Cyber Security Requirements

Cyber security is a high priority for TRUMPF and TRUMPF makes considerable efforts to create and maintain an adequate level of protection for information and data. Consequently, TRUMPF requires an adequate level of cyber security from suppliers. The requirements for suppliers are described in this document and the contractor is obligated to comply with them.

A. General section: General requirements for suppliers

1. Product-related requirements

1.1. The following applies to hardware and software purchase contracts:

The supplier guarantees that the delivery item corresponds to the current state of the art at the time of the transfer of risk. This includes, e.g. protection against malware (e.g. Trojans, viruses, spyware, etc.), information security and data-backup measures, compliance with applicable data protection requirements for software and all precautions and measures according to the currently recognized state of ICT technology. The supplier guarantees that the delivery item is safeguarded by suitable technical protection and hardening measures in the best possible way according to the current state of the art and that this has been demonstrably done by appropriate technical tests by the supplier [such as the following requirements for a technical inspection: static code analysis (SAST), vulnerability analyses with vulnerability scanners (DAST) and/or a correct processing of input data into the software with the help of fuzzing / robustness testing]. In addition, in the case of software products, the supplier must provide TRUMPF with a software bill of materials (SBOM) in which all third-party software (sub-)components contained in the software are listed, in particular open-source software. The supplier warrants to TRUMPF that the list of third-party software is up to date at the time of the hardware/software delivery to TRUMPF.

1.2. In all other respects, the following applies:

The supplier shall observe the current state of the art in the provision of services. This includes, e.g. protection against malware (e.g. Trojans, viruses, spyware, etc.), information security and data-backup measures, compliance with applicable data protection requirements for software and all precautions and measures according to the currently recognized state of ICT technology. Every new update, upgrade, release or otherwise new version of software is safeguarded by the supplier before delivery, using a suitable technical protection and hardening measures in the best possible way according to the current state of the art and this is demonstrably done by appropriate technical tests by the supplier [such as the following requirements for a technical inspection: static code analysis (SAST), vulnerability analyses with vulnerability scanners (DAST) and/or a correct processing of input data into the software with the help of fuzzing / robustness testing].

2. Organizational requirements

2.1. The supplier is obliged:

a. to implement a secure software development lifecycle if the contractual services involve the transfer or making available of software. This includes the continuous training of software developers on security-related aspects of software development;

b. to maintain vulnerability management and at least (1) continuously check its contractual products and services for information security or data protection vulnerabilities and inform TRUMPF immediately of discovered information security or data protection vulnerabilities and to assess them according to valid standard metrics (e.g. CVSS), to report this to cybersecurity.external@trumpf.com and remedy them within the agreed deadlines, or otherwise within a reasonable period of time, and (2) locate and analyze information security or data protection vulnerabilities communicated by TRUMPF or third parties and remedy them within the agreed deadlines, or otherwise within a reasonable period of time;

2.2. TRUMPF is entitled to demand proof of compliance with the above obligations and proof of information security such as e.g. certificates, results of penetration or vulnerability tests at least once a calendar year.

2.3. Furthermore, the supplier is obliged to report to TRUMPF significant changes with an impact on information security, such as technology changes or the withdrawal/expiry of certificates. In the event that this results in significant negative effects on the level of security, TRUMPF is entitled to withdraw from the contract extraordinarily.

2.4. The supplier is to hand over to TRUMPF the processed information, all necessary documents and, if necessary, software created on behalf of TRUMPF in an agreed format and within an appropriate time if the continuation of the service provision is not guaranteed. This is particularly the case if the supplier is no longer able to provide products or services.

2.5. To the extent permitted by law, the supplier is to legally exhaust any statutory recourse before customer data is passed on. In addition, unless it is strictly prohibited, the supplier is to inform TRUMPF about this transfer and ask for consent.

2.6. The supplier obliges its subcontractors to comply with all the aforementioned requirements in the entire process chain accordingly.

2.7. The provisions in this appendix do not in any case limit the other agreed contractual obligations of the supplier.

B. Special section: Requirements for suppliers in addition to the general section on specific organization-related / different supplier categories

The validity for the organizational requirements is divided into three different supplier categories, which are described below and identified in the following numbers by the defined abbreviations:

1. Full managed services (FS): The supplier provides the service within the framework that it defines (locations, hardware, software, processes and technical concepts). The supplier may integrate further IT service providers for the provision of services to the customer (relocation to subcontractors). The contractor's information security management system (ISMS) shall apply to the object of service.

For example: The provision of software-as-a-service solutions (e.g. MS Office 365)

2. Remote managed services (RS): The supplier provides services in TRUMPF locations or through third parties commissioned by TRUMPF. The supplier accesses the IT infrastructure at TRUMPF via an IT infrastructure managed by the supplier (remote access). Access is provided in accordance with the procedures provided by TRUMPF. The services are provided in accordance with TRUMPF's guidelines, operating processes, technical concepts and within TRUMPF's information security management system (ISMS).

For example: The administration of the IT-infrastructure components (OnPrem or Cloud)

3. Support services (SS): The supplier provides a service within the framework of a consulting contract or maintenance contract for hardware/software and receives confidential data from TRUMPF for the provision of services. The processing and storage of confidential TRUMPF data takes place in the supplier's IT infrastructure in accordance with its information security management system (ISMS).

For example: Management consulting, software maintenance with error analyses / remote maintenance, profitability calculations, market analyses, other processing of confidential or business critical information from TRUMPF

The supplier is obliged:

a. to maintain an information security management system (ISMS) in accordance with ISO 27000 et seq. or equivalent standards [FS/RS/SS];

b. to secure TRUMPF information, the IT systems necessary for the contractual performance, and the data transmissions by means of appropriate protective

measures that observe the current state of the art and comply with the least-privilege and need-to-know principles [FS/RS/SS];

c. to secure network access from the Internet using a strong authentication (e.g. multi-factor authentication). Access protection passwords must enforce appropriate rules for length and complexity [FS/RS/SS];

d. in the event of information security incidents that affect TRUMPF's corporate assets protection objectives, (1) to inform TRUMPF (cybersecurity.external@trumpf.com) immediately of detected security incidents, (2) in the event of imminent danger to take suitable and appropriate measures to safeguard from danger the protection objectives for TRUMPF's corporate assets, (3) to document the measures taken in the context of a security incident in a comprehensible manner and to provide the documentation to TRUMPF upon request, (4) to coordinate the publication of information on a security incident with TRUMPF and (5) in the event of suspicious behavior or inexplicable failures of the supplier's systems, where TRUMPF data is also stored, to intervene immediately on the systems and, if necessary, to carry out subsequent forensic investigations. Any logs for security-relevant events on the supplier's systems are to be stored centrally, and (6) the supplier is to notify immediately of requests from public authorities for information on or for the transmission of company assets and to coordinate the further course of action [FS/RS/SS];

e. to train its employees at least once a calendar year regarding threats, and the protective measures and behavior needed for the secure handling of information [FS/RS/SS];

f. to coordinate and contractually agree with TRUMPF on the responsibilities, cooperation obligations and provision obligations necessary for the provision of services [FS/RS/SS];

g. to coordinate and contractually agree on the data backup and recovery processes. At least the recovery point objective (RPO) and recovery time objective (RTO) must be defined. If the contractual service is used in TRUMPF business processes that are based on at least high availability requirements, the recovery processes and emergency processes must be tested at least once a calendar year and TRUMPF must be provided with suitable proof of this [FS/RS];

h. to carry out the data processing and storage of TRUMPF information only in suitable premises with physical protective measures that offer adequate protection against environmental influences and entrance/access by unauthorized third parties [FS/SS];

i. to maintain a central log management with a continuous evaluation of security-relevant protocols that monitors the confidentiality and integrity of the information if TRUMPF information is processed and stored on the supplier's systems [FS/SS];

j. to have server rooms that comply with protection and availability class 3 of DIN EN 50600 in the currently valid version if the contractual service is used in TRUMPF business processes that are based on at least high availability requirements [FS];

k. to maintain a reporting system on customer-relevant information security risks that meets the following requirements: (1) provision over a regular reporting cycle, reporting at least once a calendar year, with an overview of the (2) identified customer-relevant risks and their measures; (3) the execution of security audits (e.g. penetration tests); (4) the implementation of security awareness measures [FS].