TRUMPF

TRUMPF Cyber Security Requirements	Requisiti di sicurezza informatica TRUMPF
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.	La sicurezza informatica ha la massima priorità per TRUMPF e TRUMPF compie sforzi considerevoli per creare e salvaguardare un adeguato livello di protezione per informazioni e dati. Di conseguenza, TRUMPF esige un adeguato livello di sicurezza informatica da parte dei fornitori. Il presente documento descrive i requisiti per i fornitori e il contraente è tenuto a osservarli.
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.	**Sezione generale: Requisiti generali per i fornitori** **1. Requisiti legati al prodotto** **1.1** Ai contratti d'acquisto per hardware e software si applica quanto segue: Il fornitore garantisce che l'oggetto della fornitura corrisponde all'attuale stato della tecnica al momento del trasferimento del rischio. Questo comprende ad esempio la protezione dal malware (ad es. trojan, virus, spyware, ecc.), le misure di sicurezza informatica e per il back up dei dati, il rispetto dei requisiti di protezione dei dati applicabili ai software e tutte le precauzioni e le misure previste dall'attuale livello riconosciuto delle tecnologie dell'informazione e della comunicazione. Il fornitore garantisce che l'oggetto della fornitura è dotato di idonee misure di protezione tecnica e di hardening nel miglior modo possibile secondo l'attuale stato della tecnica e che questo è stato dimostrato dal fornitore mediante opportune prove tecniche [come ad esempio i seguenti requisiti per un'ispezione tecnica: test statico della sicurezza delle applicazioni (SAST), analisi della vulnerabilità condotte con vulnerability scanner (DAST) e/o una corretta elaborazione dei dati in ingresso nel software con l'aiuto di fuzzing/test di robustezza]. Inoltre, nel caso di prodotti software, il fornitore deve fornire a TRUMPF una distinta base del software (SBOM) che elenchi tutte le (sotto)componenti di software di terzi contenute nel software, in particolare software open-source. Il fornitore garantisce a TRUMPF che l'elenco dei software di terzi è aggiornato al momento della consegna dell'hardware/software a 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].	**1.2** Per tutti gli altri aspetti, vale quanto segue: Il fornitore deve rispettare l'attuale stato della tecnica nella fornitura dei servizi. Questo comprende ad esempio la protezione dal malware (ad es. trojan, virus, spyware, ecc.), le misure di sicurezza informatica e per il back up dei dati, il rispetto dei requisiti di protezione dei dati applicabili ai software e tutte le precauzioni e le misure previste dall'attuale livello riconosciuto delle tecnologie dell'informazione e della comunicazione. Ogni nuovo aggiornamento, upgrade, release o altre nuove versioni del software sono protetti dal fornitore prima della consegna mediante idonee misure di protezione tecnica e di hardening nel miglior modo possibile secondo l'attuale stato della tecnica; questo è dimostrato dal fornitore mediante opportune prove tecniche [come ad esempio i seguenti requisiti per un'ispezione tecnica: test statico della sicurezza delle applicazioni (SAST), analisi della vulnerabilità condotte con vulnerability scanner (DAST) e/o una corretta elaborazione dei dati in ingresso nel software con l'aiuto di fuzzing/test di robustezza].
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	**3. Requisiti organizzativi** **2.1** Il fornitore è tenuto: a. A implementare un ciclo di vita dello sviluppo di software sicuro qualora i servizi previsti dal contratto implichino il trasferimento o la messa a disposizione del software. A tale fine è necessaria una continua formazione degli sviluppatori di software sugli aspetti legati alla sicurezza dello sviluppo dei software. b. A mantenere una gestione delle vulnerabilità e almeno (1) di controllare in modo continuativo i propri prodotti e servizi previsti dal contratto per verificarne le vulnerabilità nella sicurezza informatica e nella protezione dei dati, e a informare TRUMPF senza indugio qualora si dovessero rilevare vulnerabilità nella sicurezza informatica o nella protezione dei dati, e inoltre a valutarle in base a valide metriche standard (ad es. CVSS), a riferirle a cybersecurity.external@trumpf.com e a porvi rimedio entro i termini concordati, o altrimenti entro un ragionevole intervallo di tempo, e (2) individuare e analizzare le vulnerabilità nella sicurezza informatica o nella protezione dei

deadlines, or otherwise within a reasonable period of time;	dati comunicate da TRUMPF o da terzi e a porvi rimedio entro i termini concordati, o altrimenti entro un ragionevole intervallo di tempo;
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.	**2.2** TRUMPF ha facoltà di richiedere una prova del rispetto degli obblighi di cui sopra e la prova della sicurezza informatica, come ad es. certificati, risultati di penetration test o test di vulnerabilità almeno una volta in un anno solare.
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.	**2.3** Inoltre il fornitore si impegna a segnalare a TRUMPF eventuali importanti modifiche che abbiano effetto sulla sicurezza informatica, come ad esempio modifiche tecnologiche o il ritiro/la scadenza dei certificati. Qualora questo comporti significativi effetti negativi sul livello di sicurezza, TRUMPF ha facoltà di ritirarsi dal contratto in via eccezionale.
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.	**2.4** Il fornitore dovrà consegnare a TRUMPF le informazioni elaborate, tutti i documenti necessari e, se necessario, i software creati su incarico di TRUMPF nel formato convenuto ed entro un intervallo di tempo adeguato qualora non sia possibile garantire la prosecuzione della fornitura del servizio. Ciò vale in particolar modo qualora il fornitore non sia più in grado di fornire prodotti o servizi.
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.	**2.5** Nella misura consentita dalla legge, il fornitore dovrà aver portato legalmente a compimento eventuali iter legali prima di trasmettere ad altri i dati del cliente. Inoltre, a meno che non sia espressamente vietato, il fornitore dovrà informare TRUMPF in merito a tale trasmissione dei dati e richiederne il consenso.
2.6 The supplier obliges its subcontractors to comply with all the aforementioned requirements in the entire process chain accordingly.	**2.6** Il fornitore obbligherà i subcontraenti a rispettare tutti i requisiti precedentemente menzionati nell'intera filiera di processo.
2.7 The provisions in this appendix do not in any case limit the other agreed contractual obligations of the supplier.	**2.7** Le disposizioni di cui alla presente appendice non limitano in alcun modo gli altri obblighi contrattuali concordati per il fornitore.
B. Special section: Requirements for suppliers in addition to the general section on specific organization-related / different supplier categories	**B. Sezione speciale: Requisiti per i fornitori che integrano la sezione generale per determinate categorie di fornitori legate all'organizzazione/categorie di fornitori diverse.**

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	La validità dei requisiti organizzativi si divide in tre diverse categorie di fornitori che sono di seguito descritte e identificate dai commi successivi mediante le abbreviazioni qui definite: 1. **Servizi completamente gestiti (FS):** Il fornitore eroga il servizio entro il quadro che ha definito (sedi, hardware, software, processi e concetti tecnici). Il fornitore può coinvolgere ulteriori fornitori di servizi informatici per l'erogazione di servizi al cliente (trasferimento a subcontraenti). All'oggetto del servizio si applicherà il sistema di gestione della sicurezza delle informazioni (ISMS) del contraente. Ad esempio: L'erogazione di soluzioni software-as-a-service (ad es. MS Office 365) 2. **Servizi gestiti da remoto (RS**): Il fornitore eroga servizi nelle sedi TRUMPF o mediante terzi incaricati da TRUMPF. Il fornitore accede all'infrastruttura informatica di TRUMPF mediante un'infrastruttura informatica gestita dal fornitore (accesso remoto). L'accesso avviene in conformità con le procedure previste da TRUMPF. I servizi sono erogati in conformità con le linee guida, le procedure operative, i concetti tecnici di TRUMPF e nell'ambito del sistema di gestione della sicurezza delle informazioni (ISMS) di TRUMPF. Ad esempio: L'amministrazione delle componenti dell'infrastruttura informatica (OnPrem o Cloud) 3. **Servizi di supporto (SS):** Il fornitore eroga un servizio nel quadro di un contratto di consulenza o manutenzione per hardware/software e riceve da TRUMPF dati riservati ai fini dell'erogazione dei servizi. L'elaborazione e l'archiviazione di dati riservati di TRUMPF ha luogo presso l'infrastruttura informatica del fornitore in conformità con il suo sistema di gestione della sicurezza delle informazioni (ISMS). Ad esempio: Consulenza sulla gestione, manutenzione dei software con analisi degli errori/manutenzione da remoto, calcoli di redditività, analisi di mercato, altre elaborazioni di informazioni riservate o critiche per l'azienda di 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, in the event of imminent danger to take suitable and appropriate measures to safeguard from danger the protection objectives for TRUMPF's corporate assets, 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];	Il fornitore è tenuto: a. A mantenere un sistema di gestione della sicurezza delle informazioni (ISMS) in conformità con ISO 27000 e successivi oppure standard equivalenti [FS/RS/SS]; b. A proteggere le informazioni di TRUMPF, i sistemi informatici necessari per lo svolgimento dell'attività prevista dal contratto e la trasmissione di dati mediante appropriate misure protettive che rispondono all'attuale stato della tecnica e sono conformi ai principi del privilegio minimo e del need-to-know [FS/RS/SS]; c. A proteggere l'accesso alla rete da internet servendosi di un'autenticazione forte (ad es. autenticazione a più fattori). Le password che proteggono l'accesso devono seguire opportune regole di lunghezza e complessità [FS/RS/SS]; d. in caso di incidenti che riguardano la sicurezza informatica e che hanno un impatto sugli obiettivi di protezione dei valori aziendali di TRUMPF, (1) a informare senza indugio TRUMPF (cybersecurity.external@trumpf.com) in merito agli incidenti di sicurezza rilevati, nell'eventualità di un pericolo imminente, ad adottare idonee e opportune misure per proteggere da tale pericolo gli obiettivi di protezione dei valori aziendali di TRUMPF, a documentare le misure adottate nel contesto di un incidente di sicurezza in modo comprensibile e a fornire la documentazione a TRUMPF qualora venga richiesto, (4) a coordinare la divulgazione di informazioni su un incidente di sicurezza con TRUMPF e (5) in caso di comportamenti sospetti oppure di guasti inspiegabili ai sistemi del fornitore in cui siano archiviati anche i dati di TRUMPF, a intervenire senza indugio sui sistemi e, se necessario, a condurre le successive indagini forensi. Tutti i registri che riguardino eventi rilevanti ai fini della sicurezza nei sistemi del fornitore devono essere archiviati a livello centrale e (6) il fornitore dovrà comunicare senza indugio eventuali richieste da parte delle pubbliche autorità di informazioni concernenti la trasmissione di valori aziendali o finalizzate a questa e a coordinare i successivi interventi [FS/RS/SS]; e. a formare i propri collaboratori almeno una volta per ogni anno solare in merito a eventuali minacce, misure protettive e comportamenti necessari per garantire una gestione sicura delle informazioni [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].	f. a coordinare e stipulare mediante contratto con TRUMPF le responsabilità, gli obblighi di collaborazione e gli obblighi di fornitura necessari all'erogazione dei servizi [FS/RS/SS]; g. a definire e a stipulare mediante contratto i processi di back-up dei dati e di recupero dati. È necessario definire almeno il punto di ripristino prefissato (RPO) e il tempo massimo di ripristino (RTO). Se il servizio previsto dal contratto viene utilizzato per i processi aziendali di TRUMPF che si basano almeno su requisiti di alta disponibilità, i processi di recupero e i processi di emergenza devono essere testati almeno una volta ogni anno solare e si deve fornire a TRUMPF una prova idonea che questi test sono stati effettuati [FS/RS]; h. a condurre l'elaborazione e l'archiviazione di dati riferiti alle informazioni di TRUMPF soltanto in locali idonei, dotati di misure protettive fisiche che offrono una protezione adeguata dalle influenze ambientali e dall'ingresso/accesso da parte di personale non autorizzato [FS/SS]; i. qualora le informazioni di TRUMPF siano elaborate e archiviate nei sistemi del fornitore [FS/SS], a monitorare la riservatezza e l'integrità delle informazioni mediante un registro centrale con valutazione continua dei protocolli rilevanti ai fini della sicurezza; j. qualora il servizio previsto dal contratto sia usato nei processi aziendali di TRUMPF che si basano almeno su requisiti di alta disponibilità [FS], ad avere sale server conformi alla classe di protezione e di disponibilità 3 di DIN EN 50600 nella versione attualmente in vigore; k. a mantenere un sistema di reporting sui rischi di sicurezza per le informazioni rilevanti per il cliente che soddisfi i seguenti requisiti: (1) fornitura di un ciclo di reporting regolare, almeno una volta per anno solare, con una panoramica di (2) rischi identificati rilevanti per il cliente e delle relative misure; (3) audit di sicurezza svolti (ad es. penetration test); (4) misure di sensibilizzazione alla sicurezza adottate [FS].