Cyber Security Bedingungen für Lieferanten
Cyber Security Terms for Suppliers

MTQ 5014

Englische Fassung ab Seite 7 / English version from page 7

Erstausgabe

Inhaltsverzeichnis Seite

CONTENTS Page

Fortsetzung Seite 2 bis 12
Continued on pages 2 to 12

Fachbereich:	Redaktionell geprüft:	Freigegeben:	ICS-Nr.
Specialist department:	Editorially checked by:	Approved by:	ICS-No.
Daniel, TEXY	Koch, TQCD	Steinhauser, TQCD	25.040.40, 35.110

1 Anwendungsbereich

Dieser Standard beschreibt grundlegende rechtliche und organisatorische Anforderungen an die Informationssicherheit für Lieferanten, Entwicklungsdienstleister und Partner (nachfolgend Auftragnehmer, AN genannt).

Dementsprechend kann er bei Lastenheften, Projektverträgen und Bestellungen herangezogen und referenziert werden, so dass er Vertragsbestandteil wird.

Abweichende Regelungen zu diesem Dokument bedürfen gesonderter schriftlicher Vereinbarung zwischen Auftragnehmer und RRS (nachfolgend Auftraggeber, AG genannt) vor einer Beauftragung.

Der Standard beschreibt keine Geheimhaltungspflichten, entsprechende Vereinbarungen zwischen Auftragnehmer und Auftraggeber müssen gesondert in einem NDA getroffen werden.

2 Normative Verweisung

Soweit projektspezifisch nichts anderes vorgegeben finden insbesondere folgende Normen / Standards branchenspezifisch Anwendung:

- IEC 62443
- ISO/IEC 2700x (Normenreihe, IT-Sicherheit)
- Stand der Technik (z.B. BSI Richtlinien)

3 Zweck

Der Standard ist insbesondere einzuhalten von Lieferanten von komplexen, softwarebasierten, elektronischen Zukaufkomponenten wie Steuergeräten, Netzwerkkomponenten, Industrierechnern, speicherprogrammierbaren Steuerungen oder ähnlichem sowie von kritischen Bauteilen und Baugruppen.

4 Mitgeltende Unterlagen

[1] Lieferantenselbstauskunft Produkt-Cybersicherheit

5 Organisation und Informationssicherheitsmanagement

Der AN ist dazu verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) zu betreiben.

1. Das Informationssicherheitsmanagement muss hierbei auch die IT-Sicherheit der IT-Infrastruktur des AN sowie die Angriffssicherheit seiner Vertragsprodukte (Produkt-Cybersicherheit) abdecken. Das ISMS des AN findet Anwendung in allen Unternehmensbereichen und an allen Standorten in denen Vertragsprodukte für den AG entwickelt, hergestellt oder gewartet werden.

   Insbesondere sollen im ISMS die Prozesse für eine Risiko- und Bedrohungsanalyse sowie ein Konzept zur unverzüglichen Reaktion auf Zwischenfälle nebst einer zeitnahen Wiederherstellung (Recovery) eines angemessenen Sicherheitsniveaus enthalten sein.

2. Der AN sichert zu und gewährleistet, dass er die geltenden Gesetze, Vorschriften und Industriestandards in Bezug auf die IT-Sicherheit kennt, insbesondere diejenigen, die sich auf das Hacken von IT oder OT-Systemen, den unrechtmäßigen Zugriff auf ein IT oder OT-System, die absichtliche Störung des IT-Systembetriebs und die missbräuchliche Verwendung von Daten beziehen, und verpflichtet sich, diese einzuhalten.

3. Der AN ist verpflichtet, die Lieferantenselbstauskunft zu Produkt-Cybersicherheit auszufüllen und die Compliance zu den Anforderungen in der Lieferantenselbstauskunft zu dokumentieren. Falls Abweichungen zu den Anforderungen vorhanden sind, werden diese dokumentiert, mit dem AG abgestimmt und proaktiv aufgelöst.

4. Der AN benennt eine verantwortliche Person als Ansprechpartner für Produkt-Cybersicherheit für die vom AG verwendeten Vertragsprodukte des AN. Eine Änderung des Verantwortlichen ist dem AG umgehend mitzuteilen.

5. Der AN dokumentiert bekannte Bedrohungen und Risiken für das Vertragsprodukt und stellt diese dem AG bereit.

6. Der AN verpflichtet sich, auf Verlangen des AG, ein Escrow-Agreement über alle Bestandteile (Software, Keys, Tools, Entwicklungsumgebung, Entwicklungsdokumente, HW-Layouts usw.) abschließen. Es ist der Nachweis der Vollständigkeit aller Vertragsprodukt- und Entwicklungsbestandteile, die durch das Escrow-Agreement erfasst werden durch den AN zu führen und dem AG in dokumentierter Form zu übergeben.

7. Der AN stellt dem AG ein Verzeichnis der in seinem Vertragsprodukt verwendeten Open Source Software und die entsprechenden Lizenzbedingungen zur Verfügung. Alle verwendeten (nicht selbstentwickelten) SW Bibliotheken, Tools, Entwicklungsumgebungen usw. müssen mit Versionsstand dokumentiert werden.

8. Auf Nachfrage liefert der AN eine Softwarestückliste (Software Bill of Material, SBOM) mit den Informationen nach einem anerkannten SBOM Standard, z.B. Software package data exchanbe format SPDX).

9. Der AN verpflichtet sich, zu jedem Vertragsprodukt ein Verzeichnis der gelieferten Hardware mit der zugehörigen Software und Versionen zu pflegen und dem AG zur Verfügung zu stellen. Falls Software unabhängig von einem Vertragsprodukt geliefert wird, so liefert der AN den Hash der Software mit.

10. Falls der AN Geheimnisse wie Passwörter oder Zugangsdaten liefert, so sind diese über einen gesonderten, vereinbarten Kanal bereit zu stellen. Die Lieferung und Dokumentation von Passwörtern und Zugangsdaten in Handbüchern ist nicht gestattet.

11. Der AN bestätigt, dass sein Vertragsprodukt nach einem anerkannten Standard der IT oder OT-Sicherheit, z.B. IEC 62443-4-1 entwickelt wurde, wobei ein strukturierter, sicherer Entwicklungsprozess einschließlich Konfigurationsmanagement und Qualitätssicherung zugrunde liegt. Auf Anfrage liefert der AN entsprechende Nachweisdokumente.

6 Audits und Sicherheitsanalysen

1. Der AG behält sich vor, ein Security-Audit für die angewendeten Prozesse der Organisation und der Projekte des AN vor Ort durchzuführen. Der AG kann damit auch Dritte beauftragen, die in seinem Namen dieses Audit durchführen. Falls vom AN gewünscht, kann das Audit durch einen unabhängigen Auditor einer akkreditierten Stelle durchgeführt werden. Der Bericht des Auditors ist dem AG vollständig vorzulegen. Der AN muss Security Audits an den betroffenen Standorten innerhalb eines Monats thematisch vollumfänglich und ohne Einschränkungen der betroffenen Bereiche ermöglichen. Grundlage für Audits sind ISO 2700x oder IEC 62443-4-1.

2. Der AN wird dem AG auf dessen Verlangen hin bereits vorliegende Nachweise einer Auditierung auf Grundlage eines anerkannten Standards (z.B. nach ISO 27001, IEC 62443-4-1 oder Cyber Essentials) liefern. Die Nachweise sind vollständig zu liefern und dürfen nicht älter als ein Jahr sein.

3. Der AG behält sich vor, eine Security Analyse (z.B. Technisches Audit, Code Review, Binäranalyse, Schwachstellenanalyse, Penetration Test) des Produktes vorzunehmen.

4. Der AN gestattet dem AG Penetrationstests oder System Penetrationstests, unter Offenlegung aller hierzu erforderlichen internen Informationen des Systems (Entwicklungsdokumente), durchzuführen. Der AG kann dazu auch Dritte beauftragen.

5. Der AN liefert dem AG die Binärsoftware zur Erstbemusterung und zu jeweiligen Updates. Der AN gestattet dem AG eine Cyber Security Binär- und Schwachstellenanalyse auf dem gelieferten Binärcode. Bei einer Binäranalyse können Geheimnisse des AN offengelegt werden, insbesondere Schwachstellen.

6. Der AN verpflichtet sich, regelmäßig Penetrationstests und Schwachstellenscans durchzuführen. Die Ergebnisse werden mit dem AG vollständig und immer geteilt. Der AN legt dem AG dar, wie und in welchem zeitlichen Rahmen die Schwachstellen behoben werden. Funktionale Tests des AN berücksichtigen das Thema Angriffssicherheit.

7 Schwachstellenmanagement

Eine Schwachstelle ist ein Fehler oder eine Schwäche im Entwurf, in der Implementierung oder im Betrieb und in der Verwaltung eines Systems, der/die (von einem Angreifer) ausgenutzt werden kann, um die Integrität oder die Sicherheit des Systems zu verletzen (siehe IEC 62443-3-2).

1. Der AN ist dazu verpflichtet ein Schwachstellenmanagement über die Laufzeit des gesamten Produktlebenszyklus zu pflegen. Das Schwachstellenmanagement beinhaltet auch eine regelmäßige, dokumentierte Analyse von Schwachstellendatenbanken und der Relevanz für die Vertragsprodukte.

2. Der AN verpflichtet sich, etwaige kritische Schwachstellen seiner Vertragsprodukte, die ihm bekannt sind oder die bekannt werden, unverzüglich zu bewerten und zu beheben.

3. Die Reaktionszeit für das Berichten von Schwachstellen nach Erkennung und Vorkommnissen an den AG durch den AN beträgt 24 Stunden, von Montag bis Freitag. Diese gilt unabhängig etwaiger Gewährleistungsfristen oder sonstiger gesetzlicher Verjährungsfristen über einen Zeitraum von 20 Jahren nach Lieferung. Für das Berichten kritischer Schwachstellen kann ein CVSS Schwellwert vereinbart werden.

4. Der AN informiert den AG unverzüglich über bekannt gewordene Schwachstellen und Zwischenfälle (Security Incidents) an Vertragsprodukten, die an den AG geliefert wurden. Dazu wird ein entsprechender Score (z.B. CVSS Score oder EPSS oder SSVC oder VPR) und das Traffic Light Protokoll verwendet.

5. Der AN verwendet zur Meldung von Schwachstellen die E-Mail Adresse PSIRT@ps.rolls-royce.com

8 Sicherheitsupdates

1. Der AN verpflichtet sich, bekannte Schwachstellen, die die Sicherheit (Produkt-Cybersicherheit) des Systems des AG beeinträchtigen, in einem angemessenen Zeitraum zu beheben. Ein angemessener Zeitraum ist < 90 Tage falls kein anderer Zeitraum mit dem AG vereinbart ist. Bei Gefahr für Leib und Leben hat der Lieferant unverzüglich alles zu tun, um die von seinem Vertragsprodukt ausgehenden Gefahren zu begegnen bzw. kompensierende (auch betriebliche) Gegenmaßnahmen zu definieren, umzusetzen und zu kommunizieren.

2. Der AN verpflichtet sich, für das System des AG Sicherheitspatches für den gesamten Vertragsproduktlebenszyklus bereitzustellen, um bekannt gewordene Schwachstellen zu schließen. Dies gilt unabhängig etwaiger Gewährleistungsfristen oder sonstiger gesetzlicher Verjährungsfristen über einen Zeitraum von 20 Jahren nach Lieferung.

3. Der AN verpflichtet sich, den AG bei End-of-Life des Vertragsproduktes mindestens 1 Jahr vor Produktionsende zu informieren. Sofern es dem AN aufgrund äußerer Umstände nicht möglich ist, spätestens 48h nach Bekanntwerden.

9 Mitwirkung des Auftragnehmers

1. Der AN verpflichtet sich, konstruktiv an der sicheren Integration seines Vertragsproduktes in das System des AG mitzuwirken.

2. Der AN verpflichtet sich, an Abstimmungen mit dem AG und dem End-Kunden teilzunehmen, sowie aktiv an der Erstellung eines gesamtheitlichen IT Sicherheitskonzeptes mitzuwirken, soweit es sein Vertragsprodukt betrifft. Ein ggf. vorhandenes IT-Sicherheitskonzept für das Vertragsprodukt ist mit dem Vertragsprodukt zu liefern. Das gesamtheitliche IT-Sicherheitskonzept bezieht sich auf den Lieferumfang des AG und kann sowohl technische Maßnahmen als auch organisatorische und personelle Maßnahmen beinhalten.

3. Der AN verpflichtet sich, auf Anfrage des AG eine Security Analyse des Vertragsproduktes zusammen mit dem AG, bei Bedarf, vorzunehmen. Insbesondere unterstützt der AN den AG bei der technischen Bewertung seines Vertragsproduktes gegenüber IEC 62443-4-2.

4. Wenn der AN von einem tatsächlichen Vorfall innerhalb seiner IT Infrastruktur erfährt, die eine tatsächliche oder potenziell nachteilige Auswirkung auf die Infrastruktur des AN haben kann, in dem Daten des AG gespeichert sind ("Cybervorfall") oder von einem sonstigen unbefugten Zugriff auf oder die Nutzung oder der Missbrauch, die Beschädigung oder die Zerstörung durch einen Dritten ("sonstiger Vorfall") erfährt , muss der Lieferant den AG unverzüglich und nicht später als 24 Stunden, nachdem er von dem Cybervorfall oder dem sonstigen Vorfall Kenntnis erlangt hat benachrichtigen.

5. Der AN verpflichtet sich, allen Anweisungen des AG im Zusammenhang mit dem Cybervorfall oder sonstigen Vorfall zu befolgen und die gesetzlichen Regelungen einzuhalten. Dies betrifft insbesondere die Beschaffung und Sicherung von Beweisen über den Cybervorfall, die Umsetzung von Abhilfestrategien, um die Auswirkungen des Cybervorfalls oder eines anderen Vorfalls oder die Wahrscheinlichkeit oder die Auswirkungen zukünftiger ähnlicher Vorfälle zu verringern und die Benachrichtigung von Behörden. Beweise sind für einen Zeitraum von 12 Monaten aufzubewahren.

6. Der Daten- und Informationsaustausch kann exportrechtlichen Einschränkungen unterliegen. Hier besteht Informationspflicht durch den Auftragnehmer.

10 Vertragsprodukthärtung und Risikomitigation

1. Der AN liefert mit dem Vertragsprodukt Hinweise zur sicheren Einstellung und Härtung des Vertragsproduktes, insbesondere für Netzwerk und/oder Betriebssystemeinstellungen.

2. Alle kryptographischen Funktionen sind nach Stand der Technik auszuführen (siehe z.B. technische Richtlinien des BSI, BSI TR-2102). Der AN bestätigt, dass er ein Verfahren implementiert, um kryptographische Schlüssel und andere Geheimnisse, die die Vertragsprodukte für den AG betreffen, nach dem Stand der Technik sicher zu schützen.

3. Ausrüstung und Verkabelung dürfen nicht mit Informationen gekennzeichnet werden, die einen Cyber-Angriff unterstützen könnten, wie z. B. Zweck des Geräts, Verbindungstypen, Kommunikationstyp, Konfigurationsdetails (z. B. IP-Adressen), Sicherheitsdetails (z. B. Logins/Passwörter), Schalterpositionsschlüssel.

4. Der AN bestätigt auf Verlangen des AG mit einem Protokoll, dass gelieferte Software zum Zeitpunkt der Auslieferung auf Malware und sonstige Schadsoftware geprüft wurde und frei von dergleichen ist.

5. Wenn spezielle Hardware oder Software für Update-Aktivitäten, Diagnose, Operation, Konfiguration oder weitere Aktivitäten am Vertragsprodukt des AN, notwendig ist, so gilt diese Hardware oder Software ebenfalls als Vertragsprodukt und muss im Lieferumfang enthalten sein. Der AN räumt dem AG und dem Kunden das permanente Recht zur Nutzung der Software ein und wartet diese über die Lebensdauer des Vertragsprodukts. Die Software wird als Installationspaket mit Release Notes und Hash geliefert. Auf Anforderung durch den AG ist der AN dazu verpflichtet nachzuweisen, nach welchen Standards die Hardware oder Software entwickelt wurde.

6. Falls Standardbetriebssysteme im Vertragsprodukt benutzt werden, so stimmt der AN mit dem AG auf Anfrage ein Patchmanagementkonzept und ein Antivirenkonzept ab und liefert dieses. Falls vereinbart, wird das Steuergerät des AN mit Antivirensoftware geliefert.

ENDE DER DEUTSCHEN FASSSUNG!

The *English* version is a translation. In case of dispute the German original will govern.

First Edition

1 Scope of application

This standard describes basic legal and organisational information security requirements for suppliers, development service providers and partners (hereinafter referred to as contractors, AN).

Accordingly, it can be referred to and referenced in specifications, project contracts and purchase orders so that it becomes part of the contract.

Deviating regulations to this document require a separate written agreement between the contractor and RRS (hereinafter referred to as the client, AG) before an order is placed.

The standard does not describe any confidentiality obligations; corresponding agreements between contractor and client must be made separately in an NDA.

2 Normative reference

Unless otherwise specified for a specific project, the following norms/standards in particular shall apply to the industry:

- IEC 62443
- ISO/IEC 2700x (series of standards, IT security)
- State of the art (e.g. BSI guidelines)

3 Purpose

The standard is to be complied with in particular by suppliers of complex, software-based, electronic bought-in components such as control units, network components, industrial computers, programmable logic controllers or similar, as well as critical components and assemblies.

4 Applicable documents

[1] Supplier Self-Assessment on Product Cyber Security

5 Organisation and information security management

The Contractor is obliged to operate an information security management system (ISMS).

1. The information security management must also cover the IT security of the Contractor's IT infrastructure and the attack security of its contractual products (product cyber security). The ISMS of the Contractor shall be applied in all divisions and at all locations where contractual products are developed, manufactured or maintained for the Client.

   In particular, the ISMS shall contain the processes for threat and risk analysis as well as a concept for immediate reaction to incidents together with a timely recovery of an appropriate security level.

2. The Contractor represents and warrants that he is aware of and undertakes to comply with applicable laws, regulations and industry standards relating to IT security, in particular those relating to hacking of IT or OT systems, unlawful access to an IT or OT system, intentional disruption of IT system operations and misuse of data.

3. The Contractor is obliged to complete the Supplier Self-Assessment on Product Cyber Security and to document compliance with the requirements in the Supplier Self-Assessment. If there are deviations from the requirements, these are to be documented, coordinated with the Client and proactively resolved.

4. The Contractor shall appoint a responsible person as contact person for product cyber security for the Contractor's contractual products used by the Client. The Client shall be informed immediately of any change in the person responsible.

5. The Contractor shall document known threats and risks to the contractual product and make them available to the Client.

6. The Contractor undertakes to conclude an escrow agreement for all components (software, keys, tools, development environment, development documents, hardware layouts, etc.) at the Client's request. The Contractor shall provide proof of the completeness of all contractual product and development components covered by the escrow agreement and hand them over to the Client in documented form.

7. The Contractor shall provide the Client with a list of the open source software used in its contractual product and the corresponding licence conditions. All (not self-developed) software libraries, tools, development environments etc. used must be documented with the version status.

8. Upon request, the Contractor shall provide a software bill of material (SBOM) with the information according to a recognised SBOM standard, e.g. software package data exchange format SPDX).

9. The Contractor undertakes to maintain a list of the hardware supplied with the associated software and versions for each contractual product and to make this available to the Client. If software is supplied independently of a contractual product, the Contractor shall also supply the hash of the software.

10. If the Contractor supplies secrets such as passwords or access credentials, these shall be provided via a separate, agreed channel. The delivery and documentation of passwords and access credentials in manuals is not permitted.

11. The Contractor confirms that its contractual product was developed in accordance with a recognised standard of IT or OT security, e.g. IEC 62443-4-1, based on a structured, secure development process including configuration management and quality assurance. Upon request, the Contractor shall provide corresponding evidence documents.

6 Audits and security analyses

1. The Client reserves the right to carry out a security audit for the applied processes of the Contractor's organisation and projects on site. The Client may also commission third parties to carry out this audit on its behalf. If desired by the Contractor, the audit may be carried out by an independent auditor of an accredited body. The auditor's report shall be submitted in full to the Client. The Contractor must allow security audits to be carried out at the affected locations within one month, fully covering the subject matter and without any restrictions on the affected areas. Basis for audits are ISO 2700x or IEC 62443-4-1.

2. At the Client's request, the Contractor shall provide the Client with existing evidence of an audit based on a recognised standard (e.g. in accordance with ISO 27001, IEC 62443-4-1 or Cyber Essentials). The evidence shall be provided in full and shall not be older than one year.

3. The Client reserves the right to carry out a security analysis (e.g. technical audit, code review, binary analysis, vulnerability analysis, penetration test) of the product.

4. The Contractor shall allow the Client to carry out penetration tests or system penetration tests, disclosing all internal system information (development documents) required for this purpose. The Client may also commission third parties for this purpose.

5. The Contractor shall deliver the binary software to the Client for initial sampling and for respective updates. The Contractor shall allow the Client to perform a cyber security binary and vulnerability analysis on the binary code supplied. During a binary analysis, secrets of the Contractor may be disclosed, in particular vulnerabilities.

6. The Contractor carries out regular penetration tests and vulnerability scans. The results shall always be shared with the Client in full. The Contractor shall explain to the Client how and in what time frame the vulnerabilities will be remedied. Functional tests of the Contractor shall take into account the issue of attack security.

7 Vulnerability management

A vulnerability is a flaw or weakness in the design, implementation or operation and management of a system that can be exploited (by an attacker) to violate the integrity or security of the system (see IEC 62443-3-2).

1. The Contractor is obliged to maintain a vulnerability management system throughout the entire product life cycle. The vulnerability management also includes a regular, documented analysis of vulnerability databases and the relevance for the contractual products.

2. The Contractor undertakes to immediately assess and remedy any critical vulnerabilities of its contractual products that are known to it or that become known to it.

3. The response time for reporting vulnerabilities after detection and incidents to the Client by the Contractor is 24 hours, from Monday to Friday. This applies irrespective of any warranty periods or other statutory limitation periods for a period of 20 years after delivery. A CVSS threshold value can be agreed for the reporting of critical vulnerabilities.

4. The Contractor shall inform the Client without delay of any known vulnerabilities and incidents (security incidents) in contractual products delivered to the Client. For this purpose, a corresponding score (e.g. CVSS score or EPSS or SSVC or VPR) and the Traffic Light Protocol shall be used.

5. The Contractor shall use the e-mail address PSIRT@ps.rolls-royce.com to report vulnerabilities.

8 Security updates

1. The Contractor undertakes to remedy known vulnerabilities affecting the security (product cyber security) of the Client's system within a reasonable period of time. A reasonable period of time is < 90 days if no other period of time has been agreed with the Client. In the event of danger to life and limb, the Supplier shall immediately do everything in its power to counter the dangers emanating from its contractual product or to define, implement and communicate compensatory (including operational) countermeasures.

2. The Contractor undertakes to provide security patches for the Client's system for the entire contractual product life cycle in order to close any vulnerabilities that become known. This shall apply irrespective of any warranty periods or other statutory limitation periods for a period of 20 years after delivery.

3. The Contractor undertakes to inform the Client of the end-of-life of the contractual product at least 1 year before the end of production. If it is not possible for the Contractor due to external circumstances, at the latest 48 hours after becoming known.

9 Cooperation of the Contractor

1. The Contractor undertakes to cooperate constructively in the secure integration of its contractual product into the Client's system.

2. The Contractor undertakes to participate in coordination with the Client and the end customer and to actively participate in the creation of an overall IT security concept, insofar as it concerns its contractual product. Any existing IT security concept for the contractual product shall be delivered with the contractual product. The holistic IT security concept refers to the Client's scope of delivery and may include technical measures as well as organisational and personnel measures.

3. The Contractor undertakes to carry out a security analysis of the contractual product together with the Client, if required, at the Client's request. In particular, the Contractor shall support the Client in the technical evaluation of its contractual product against IEC 62443-4-2.

4. If the Supplier learns of an actual incident within its IT infrastructure that may have an actual or potential adverse effect on the Contractor's infrastructure in which the Client's data is stored ("Cyber Incident") or of any other unauthorised access to or use or misuse, damage or destruction by a third party ("Other Incident"), the Supplier shall notify the Client immediately and no later than 24 hours after it becomes aware of the Cyber Incident or Other Incident.

5. The Contractor undertakes to comply with all instructions issued by the Client in connection with the cyber incident or other incident and to comply with the statutory regulations. This relates in particular to obtaining and preserving evidence about the cyber incident, implementing remediation strategies to reduce the impact of the cyber incident or other incident or the likelihood or impact of future similar incidents and notifying authorities. Evidence shall be retained for a period of 12 months.

6. The exchange of data and information may be subject to restrictions under export law. In this case, the contractor is obliged to provide information pro-actively.

10 Contract product hardening and risk mitigation

1. The Contractor shall supply with the Contract Product instructions for the secure setting and hardening of the Contract Product, in particular for network and/or operating system settings.

2. All cryptographic functions shall be performed according to the state of the art (see e.g. technical guidelines of the BSI, BSI TR-2102). The Contractor confirms that it implements a procedure to securely protect cryptographic keys and other secrets relating to the contractual products for the Client in accordance with the state of the art.

3. Equipment and wiring must not be labelled with information that could support a cyber-attack, such as purpose of the device, connection types, communication type, configuration details (e.g. IP addresses), security details (e.g. logins/passwords), switch location keys.

4. At the Client's request, the Contractor shall confirm by means of a protocol that the software supplied was checked for malware and other malicious software at the time of delivery and is free of such.

5. If special hardware or software is required for update activities, diagnosis, operation, configuration or other activities on the Contractor's contractual product, this hardware or software shall also be deemed to be a contractual product and must be included in the scope of delivery. The Contractor shall grant the Client and the Customer the permanent right to use the software and shall maintain it over the lifetime of the contractual product. The software shall be delivered as an installation package with release notes and hash. Upon request by the Client, the Contractor shall be obliged to provide evidence of the standards according to which the hardware or software was developed.

6. If standard operating systems are used in the contractual product, the Contractor shall agree a patch management concept and an anti-virus concept with the Client on request and shall supply these. If agreed, the Contractor's control unit shall be supplied with anti-virus software.