Anforderungen an die Informationssicherheit für Geschäftspartner
Information Security Guideline for Business Partners

MTQ 5015

Englische Fassung ab Seite 7 / English version from page 7

Erstausgabe

Inhaltsverzeichnis

1 Anwendungsbereich ... 3
2 Normative Verweisung ... 3
3 Zweck ... 3
4 Mitgeltende Unterlagen ... 3
5 Einhaltung von Vorschriften und Normen einschließlich relevanter Zertifizierungen ... 4
6 Informationssicherheits-Managementsystem (ISMS) ... 4
7 Datenschutz-Managementsystem (DSMS) ... 4
8 Sicherheitsbewusstsein ... 4
9 Sicherheit der Lieferkette ... 4
10 Umgang mit Notfallereignissen und Vorfällen ... 4
11 Physische Sicherheit ... 5
12 Vertrauliche Datensicherheit ... 5
13 Zugriffskontrolle und Authentifizierung für IT-Systeme und -Dienste ... 5
14 Software- und Systemsicherheit ... 5
15 IT-Netzwerksicherheit ... 6
16 Beendigung der Zusammenarbeit ... 6

Fortsetzung Seite 2 bis 10
Continued on pages 2 to 10

Fachbereich: Department:	Redaktionell geprüft: Checked:	Freigegeben: Approved:	ICS-Nr. ICS-No.
Norman Wenk, DIS	L. Thoma, OQCD	J. Mühlwerth, OQCD	25.040.40, 35.110

Rolls-Royce Solutions GmbH
Für diese Werknorm behalten wir uns alle Rechte vor
All rights reserved for this Factory standard
Exportkontrollrelevanz: nicht gelistet / Export control relevance: not listed

Table of Contents

1 Scope of application 7

2 Normative references 7

3 Purpose 7

4 Applicable documents 7

5 Compliance with regulations and standards, incl. relevant certifications 8

6 Information Security Management System (ISMS) 8

7 Data Privacy Management System (DPMS) 8

8 Security awareness 8

9 Supply chain security 8

10 Handling of emergencies and incidents 8

11 Physical security 9

12 Confidential data security 9

13 Access control and authentication for IT systems and services 9

14 Software and system security 9

15 IT network security 10

16 Termination of the cooperation 10

1 Anwendungsbereich

Dieser Standard beschreibt grundlegende Anforderungen an die Informationssicherheit und den Datenschutz für externe Geschäftspartner, Lieferanten, Entwicklungs- und Servicedienstleister sowie Partner (nachfolgend „Auftragnehmer“, AN) der Rolls-Royce Solutions GmbH (nachfolgend „Auftraggeber“, AG).
Dementsprechend kann er bei Lastenheften, Projektverträgen, Bestellungen und Rahmenverträgen herangezogen und referenziert werden, so dass er Vertragsbestandteil wird. Abweichende Regelungen zu diesem Dokument bedürfen einer gesonderten schriftlichen Vereinbarung zwischen AN und AG vor einer Beauftragung.
Dieser Standard beschreibt keine Geheimhaltungspflichten; entsprechende Vereinbarungen zwischen AN und AG werden gesondert in einer Geheimhaltungsvereinbarung (NDA) getroffen. Soweit personenbezogene Daten im Auftrag verarbeitet werden, sind die Anforderungen der DSGVO durch einen Vertrag zur Verarbeitung personenbezogener Daten (Auftragsverarbeitungsvertrag) zu konkretisieren.

2 Normative Verweisung

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

- ISO/IEC 27001 bzw. ISO/IEC 2700x (Normenreihe, Informationssicherheit)
- NIST Cybersecurity Framework (CSF) 2.0
- Stand der Technik (z. B. einschlägige BSI-Richtlinien)
- Anwendbare gesetzliche und regulatorische Anforderungen an Informationssicherheit und Datenschutz (je Branche/Region)

3 Zweck

Zweck dieses Standards ist es, sicherzustellen, dass Informationen, Daten und IT-Systeme des AG sowie AG-relevante Informationen, Daten und IT-Systeme beim AN im Rahmen der Leistungserbringung angemessen geschützt werden. Der Schutz umfasst insbesondere Vertraulichkeit, Integrität und Verfügbarkeit sowie die Einhaltung von Datenschutzanforderungen.

4 Mitgeltende Unterlagen

- Geheimhaltungsvereinbarung (NDA) zwischen AN und AG (projektspezifisch)
- Auftragsverarbeitungsvertrag (sofern einschlägig)
- Projekt-/Vertragsdokumente (Lastenheft, Projektvertrag, Bestellung), soweit auf diesen Standard referenziert wird

5 Einhaltung von Vorschriften und Normen einschließlich relevanter Zertifizierungen

Der AN stellt sicher, dass alle Standards, Richtlinien und Vorgaben zur Informationssicherheit und zum Datenschutz innerhalb der eigenen IT sowie über alle relevanten Geschäftsbereiche und Geschäftsprozesse hinweg eingehalten werden. Dies umfasst die für die jeweilige Branche und/oder Region relevanten regulatorischen Anforderungen an Informationssicherheit und Datenschutz sowie die Ausrichtung an international anerkannten Standards wie ISO/IEC 27001 und NIST CSF 2.0.
Die Konformität ist regelmäßig zu überprüfen und zu auditieren, um sicherzustellen, dass sie in der IT- und Geschäftsprozessumgebung des AN auf dem neuesten Stand ist. Wenn gesetzliche Anforderungen dies erfordern, müssen Informationssicherheitsrichtlinien und -prozesse unabhängig geprüft und zertifiziert sowie die Zertifizierung regelmäßig erneuert werden. Zumindest intern muss die Einhaltung dieser Anforderungen jährlich umfassend überprüft werden.
Sollte es in begründeten Ausnahmefällen notwendig sein, von diesen Richtlinien abzuweichen, sind die daraus resultierenden Risiken aufzulisten und mit dem AG abzustimmen. Die jeweilige Dauer einer Ausnahme ist zu bestimmen. Jede Ausnahme muss vom Head of Cyber and Information Security beim AG genehmigt werden.

6 Informationssicherheits-Managementsystem (ISMS)

Der AN betreibt ein Informationssicherheitsmanagementsystem (ISMS) einschließlich eines Kontrolllebenszyklus, um einen kontinuierlichen Überprüfungs- und Verbesserungsprozess zu gewährleisten.
Der AN implementiert ein vollständiges Asset- und Risikomanagement zumindest für AG-relevante Informationen, Daten, Produkte und Güter.

7 Datenschutz-Managementsystem (DSMS)

Der AN betreibt ein Datenschutzmanagementsystem (DSMS) einschließlich eines Kontrolllebenszyklus, um einen kontinuierlichen Überprüfungs- und Verbesserungsprozess zu gewährleisten.

8 Sicherheitsbewusstsein

Der AN stellt sicher, dass alle internen und externen Mitarbeitenden regelmäßig zu Themen und Risiken der Cyber- und Informationssicherheit sowie zum Datenschutz geschult werden.
Verdächtige Aktivitäten oder Sicherheitsvorfälle sind angemessen zu dokumentieren und zu behandeln.
Der AN stellt sicher, dass IT-Sicherheitsvorfälle, die AG-relevante Systeme oder Daten betreffen könnten, unverzüglich an die relevanten Ansprechpartner des AG gemeldet werden: informationsecurity@ps.rolls-royce.com und CyberDefenceCenter@ps.rolls-royce.com.

9 Sicherheit der Lieferkette

Der AN stellt sicher, dass die vorliegenden Sicherheitsanforderungen von allen beauftragten Lieferanten und Dienstleistern erfüllt werden, wenn sie Teil der Lieferkette für AG-relevante Aktivitäten sind.
Der AN verpflichtet alle Subunternehmer, die Zugriff auf Systeme erhalten, die AG-Daten enthalten, vertraglich zur Einhaltung der hierin dargelegten Sicherheits- und Datenschutzanforderungen. Vor jeder Verarbeitung personenbezogener Daten muss der Subunternehmer dem Auftragsverarbeitungsvertrag beigefügt werden.
Subunternehmer dürfen nur dann Zugriff auf Systeme erhalten, die AG-Daten enthalten, wenn sie zuvor schriftlich vom AG genehmigt wurden. Bei längerfristiger Zusammenarbeit ist eine laufende Überwachung des Subunternehmers und dessen Erfüllung dieser Sicherheitsanforderungen sicherzustellen.
Der AN stellt sicher, dass in den Produktionsprozessen nur Komponenten und Materialien (einschließlich Software) aus vertrauenswürdigen Quellen verwendet werden.

10 Umgang mit Notfallereignissen und Vorfällen

Der AN entwickelt Prozesse und Pläne für den Umgang und die Verarbeitung von Sicherheitsvorfällen, einschließlich Notfallplänen, die Schritte für die Wiederaufnahme der Geschäftsaktivitäten nach größeren Störungen definieren (z. B. Business Continuity/Disaster Recovery).
Der AN stellt sicher, dass alle Mitarbeitenden darin geschult sind, wie sie verdächtige Ereignisse erkennen und erkannte potenzielle Sicherheitsvorfälle melden können.

11 Physische Sicherheit

Der AN implementiert Maßnahmen, die den physischen Zugang zu Produktionsstätten und allen Einrichtungen mit potenziellem Zugriff auf geschäftskritische Informationen und personenbezogene Daten auf autorisiertes Personal beschränken.
Zutritte zu sensiblen Bereichen sind kontinuierlich zu überwachen, um sicherzustellen, dass sich keine unbefugten Personen Zutritt verschafft haben. Legitime Zutritte sind zu protokollieren.
Serverräume sind besonders zu schützen (strenge Zugangsbeschränkungen, Trennung von Büroräumen).
Besuchermanagement und -begleitung sowie allgemeine Gebäudesicherheit (z. B. Alarmanlage, Videoüberwachung, Wachpersonal) sind umzusetzen.

12 Vertrauliche Datensicherheit

Die vom AG zur Ausführung eines Auftrags zur Verfügung gestellten Daten dürfen vom AN nur zum Zwecke der Auftragserfüllung verwendet werden.
Vor jeder Verarbeitung von AG-Daten muss der AN die vom AG zur Verfügung gestellte Geheimhaltungsvereinbarung (NDA) unterzeichnet haben. Vor jeder Verarbeitung von AG-Daten, die unter die Vorschriften der DSGVO fallen, muss – sofern einschlägig – ein Vertrag zur Verarbeitung personenbezogener Daten zwischen AG und AN unterzeichnet werden.
Der AN stellt die sichere Übertragung und Speicherung von Produktionsdaten und allen anderen AG-Informationen, insbesondere vertraulichen Informationen, sicher, indem geeignete Maßnahmen zur Sicherheit von Daten beim Transport, im Ruhezustand und bei der Verwendung ergriffen werden (z. B. VPN für den Fernzugriff).
Der AN verwendet starke Verschlüsselungsverfahren, wenn Daten elektronisch übertragen oder gespeichert werden. Ist die Nutzung mobiler Datenspeicherung erforderlich, sind alle Daten zu verschlüsseln und der persönliche Gebrauch des Datenträgers auszuschließen.
Vertrauliche Papierdokumente sind sicher aufzubewahren oder sicher zu vernichten, wenn sie nicht mehr benötigt werden. Verschlusssachen sind gemäß ihrer Geheimhaltungsstufe wirksam vor unbefugtem Zugriff zu schützen.
Wo möglich sind pseudonymisierte personenbezogene Daten zu verwenden und Originaldaten getrennt zu speichern.

13 Zugriffskontrolle und Authentifizierung für IT-Systeme und -Dienste

Der AN gewährt nur solchen Mitarbeitenden Zugriff auf Systeme und Daten, die direkt an der Verarbeitung beteiligt sind (Need-to-know-Prinzip).
Jeder Zugriff oder jede Manipulation von Daten ist zu protokollieren und einer Person zuordenbar zu machen. Diese Aufzeichnungen sind automatisch zu überwachen und bei Bedarf manuell zu überprüfen.
Zugriffe dürfen nur nach einem definierten Berechtigungskonzept gewährt werden. Der AN stellt sicher, dass Konten mit Admin-Rechten keine persönlichen Konten sind, sondern technische Benutzer, auf die nur zugegriffen werden kann, wenn dies für die jeweilige Aufgabe erforderlich ist.
Der AN verwendet sichere Passwörter oder andere starke Authentifizierungsmethoden für alle Zugriffe auf IT-Systeme. Mindestanforderungen an Passwörter müssen technisch durchgesetzt werden.
Der AN stellt sicher, dass Benutzer nur die Zugriffsberechtigungen erhalten, die für ihre jeweiligen Aufgaben erforderlich sind (Least-Privilege-Prinzip). Für besonders sensible Systeme und Daten sind Multi-Faktor-Authentifizierungsverfahren umzusetzen.

14 Software- und Systemsicherheit

Der AN stellt sicher, dass in der gesamten IT, einschließlich Produktentwicklung und Fertigung, nur lizenzierte und aktuelle Software verwendet wird.
Der AN stellt sicher, dass alle Systeme in der gesamten IT, einschließlich der am Produktionsprozess beteiligten Systeme, regelmäßig mit den neuesten Sicherheitsupdates aktualisiert werden und eine aktuelle Antivirensoftware ausgeführt wird.
Entwickelt der AN eigene Software für AG-relevante Aktivitäten, sind sichere Softwareentwicklungsverfahren zu verwenden.
Der AN setzt Best Practices zur Sicherstellung der Verfügbarkeit um (z. B. Backup- & Recovery-Konzept, Antivirus, Firewall, Spam-Schutz, Serverraumüberwachung, bauliche Schutzmaßnahmen, USV, RAID, etc.).

15 IT-Netzwerksicherheit

Der AN stellt sicher, dass Produktionsnetzwerke von anderen Netzwerken getrennt sind (z. B. von Entwicklungs- und Testnetzwerken oder Netzwerksegmenten mit unterschiedlichen Sicherheitsklassifizierungen).
Zur technischen Absicherung der Netztrennung sind Firewalls und/oder andere Netzwerksicherheitssysteme wie Intrusion Detection Systeme einzusetzen.
Backups sind physisch von anderen Systemen zu trennen.

16 Beendigung der Zusammenarbeit

Bei Kündigung/Beendigung der Zusammenarbeit mit dem AG: Alle Zugriffsrechte des AN und seiner Mitarbeitenden auf Systeme mit relevanten AG-Informationen sind unverzüglich zu sperren.
Der AN stellt sicher, dass alle AG-Daten in seinen IT-Systemen gelöscht werden und physische Medien entweder an den AG übergeben oder sicher vernichtet werden, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Ergänzende Angaben

Frühere Ausgaben

Änderungen

ENDE DER DEUTSCHEN FASSUNG!

The *English* version is a translation.
The German original shall take precedence in case of dispute..

First Edition

1 Scope of application

This standard describes the basic requirements for information security and data protection applicable to external business partners, suppliers, development and service providers, and partners (hereinafter referred to as “Contractors”) of Rolls-Royce Solutions GmbH
(hereinafter referred to as the “Client”).
It can be incorporated and referenced accordingly in requirement specifications, project contracts, purchase orders, and framework agreements, thereby becoming part of the contract. Any provisions at variance from those specified in this document require a separate written agreement between the Contractor and the Client prior to assignment.
This standard does not address confidentiality obligations; any such agreements between the Contractor and the Client shall be set forth separately in a Non-Disclosure Agreement (NDA). To the extent that personal data is processed on behalf of another party, the requirements of the GDPR must be specified in a contract for the processing of personal data (data processing agreement).

2 Normative references

Unless otherwise specified for a particular project, the following industry-specific standards apply in particular:

- ISO/IEC 27001 and ISO/IEC 2700x (series of standards, information security)
- NIST Cybersecurity Framework (CSF) 2.0
- State of the art (e.g. relevant BSI guidelines)
- Applicable legal and regulatory requirements concerning information security and data protection (by industry/region)

3 Purpose

The purpose of this standard is to ensure that the information, data, and IT systems of the Client, as well as Client-related information, data, and IT systems held by the Contractor, are adequately protected throughout the course of service provision. This protection specifically includes confidentiality, integrity, and availability, as well as compliance with data protection requirements.

4 Applicable documents

- Non-Disclosure Agreement (NDA) between the Contractor and the Client (project-specific)
- Data Processing Agreement (if applicable)
- Project/contract documents (requirement specifications, project contract, purchase order), to the extent that they refer to this standard

5 Compliance with regulations and standards, incl. relevant certifications

The Contractor shall ensure compliance with all relevant standards, directives, and requirements concerning information security and data protection within its own IT systems and across all relevant business units and business processes. This includes the regulatory requirements for information security and data protection relevant to the respective industry and/or region, as well as alignment with internationally recognized standards such as ISO/IEC 27001 and NIST CSF 2.0.
Compliance must be routinely reviewed at regular intervals and audited to ensure that it remains up to date within the IT and business process environment of the Contractor. If required by law, information security policies and processes must be independently audited and certified, and certification routinely renewed at regular intervals. At the very least, compliance with these requirements must be thoroughly reviewed on an annual basis.
Should it prove necessary to deviate from these guidelines, in justifiable exceptional cases, the resultant risks shall be explicitly itemized and are contingent upon Client approval. The duration of any such exceptions shall be defined. Any exception is subject to approval by the Head of Cyber and Information Security of the Contractor.

6 Information Security Management System (ISMS)

The Contractor operates an Information Security Management System (ISMS), including a control lifecycle, to ensure a continuous and consistent process of review and improvement.
The Contractor shall implement a comprehensive Asset and Risk Management System, which applies at least to information, data, products, and goods relevant to the Client.

7 Data Privacy Management System (DPMS)

The Contractor operates a Data Protection Management System (DSMS), including a control lifecycle, to ensure a continuous and consistent process of review and improvement.

8 Security awareness

The Contractor shall ensure that all internal and external employees receive regular training on topics and risks related to cybersecurity, information security, and data protection.
Suspicious activities or security incidents shall be duly documented and addressed.
The Contractor shall ensure that any IT security incidents which might affect the systems or data of the Client are reported immediately to the designated contacts of the Client: informationsecurity@ps.rolls-royce.com and CyberDefenceCenter@ps.rolls-royce.com.

9 Supply chain security

The Contractor shall ensure that these security requirements are met by all contracted suppliers and service providers being part of the supply chain for activities relevant to the Client.
The Contractor shall require all Subcontractors granted access to systems containing data of the Client to contractually agree to comply with the security and data protection requirements set forth herein. The Subcontractor must be included in the Data Processing Agreement before any personal data is processed.
Subcontractors may only be granted access to systems containing data of the Client having first received written approval from the Client. In the case of long-term cooperation, ongoing monitoring of the Subcontractor and its compliance with these security requirements must be ensured.
The Contractor shall ensure that only components and materials (including software) from trusted sources are used in the production processes.

10 Handling of emergencies and incidents

The Contractor shall develop processes and contingency plans for managing and processing security incidents, including emergency response plans which define those steps necessary for resuming business operations following major disruptions (e.g. business continuity/disaster recovery).
The Contractor shall ensure that all employees are trained to recognize suspicious incidents and report any potential security incidents they identify.

11 Physical security

The Contractor shall implement measures to restrict physical access to production facilities and all premises with potential access to business-critical information and personal data to duly authorized personnel.
Access to sensitive areas shall be continuously monitored to ensure that no unauthorized persons have gained entry. Legitimate access shall be logged.
Server rooms shall be afforded special protection (strict access restrictions, separation from office spaces).
Visitor management and escort services, as well as general building security (e.g. alarm systems, video surveillance, security guards) shall be duly implemented.

12 Confidential data security

Data provided by the Client for the performance of a contract may be used by the Contractor solely for purposes of contract fulfillment.
Before processing any Client data, the Contractor must have signed the Non-Disclosure Agreement (NDA) provided by the Client. Where applicable, a data processing agreement shall be concluded between the Client and the Contractor before processing any Client data which falls under the provisions of the GDPR.
The Contractor shall ensure the secure transmission and storage of production data and all other Client information, in particular confidential information, by adopting appropriate measures to secure data in transit, in storage, and in use (e.g. VPN for remote access).
The Contractor shall use strong encryption methods when transmitting or storing data electronically. If the use of mobile data storage is necessary, all data must be encrypted, and any personal use of the data medium prohibited.
Confidential hardcopy documents shall be stored securely or safely destroyed when no longer needed.
Government classified information shall be effectively protected from unauthorized access in accordance with its classification.
Pseudonymized personal data is to be used wherever possible, and original data stored separately.

13 Access control and authentication for IT systems and services

The Contractor shall restrict access to systems and data to those employees directly involved in their processing (need-to-know principle).
Each and every access to or modification of data shall be logged and traceable to a specific person. These records shall be monitored automatically and verified manually as needed.
Access may only be granted in accordance with a defined authorization policy. The Contractor shall ensure that accounts with administrative privileges are not personal accounts, but rather technical user accounts that may only be accessed when necessary for a given task.
The Contractor shall use secure passwords or other strong authentication methods to restrict access to IT systems. Minimum password requirements shall be enforced by technical means.
The Contractor shall ensure that users are only granted those access rights necessary to perform their respective tasks (Principle of Least Privilege (PoLP)). Multi-factor authentication procedures shall be implemented to safeguard particularly sensitive systems and data.

14 Software and system security

The Contractor shall ensure that only licensed and up-to-date software is used throughout the IT infrastructure, including product development and manufacturing.
The Contractor shall ensure that all IT systems, including those involved in the production process, are routinely updated at regular intervals with the latest security patches and are duly protected by up-to-date antivirus software.
Contractors developing dedicated software for activities relevant to the Client shall adopt secure software development practices.
The Contractor shall implement best practices to ensure operational availability (e.g. backup and recovery plan, antivirus software, firewall, spam protection, server room monitoring, physical security measures, UPS, RAID, etc.).

15 IT network security

The Contractor shall ensure that production networks are isolated from other networks (e.g. development and test networks or network segments with differing security classifications).
Firewalls and/or other network security systems, such as intrusion detection systems, shall be used to ensure network isolation by technical means.
Backups shall be physically separated from other systems.

16 Termination of the cooperation

In the event of termination of the contract or cooperation with the Client: All access rights of the Contractor and its employees to systems containing relevant Client information shall be revoked immediately.
The Contractor shall ensure that all Client data is deleted from its IT systems and that physical media are either handed over to the Client or securely destroyed, provided that no statutory retention requirements preclude any such action.

Supplementary Information

Previous editions

Changes