Sicherheitsrichtlinie

Richtlinie für Partnerfirmen

Security Guideline

Guideline for partner companies

Überarbeitet durch / Compiled by:

S. Giske

Stand / Version:

Rev. 04 / 29.04.2024

Inhaltsverzeichnis

Sicherheitsrichtlinie: Richtlinie für Partnerfirmen

Security Guideline: Guideline for partner companies

1. Einleitung

In diesem Dokument werden die Sicherheitsanforderungen definiert, die von Dienstleistern und Lieferanten beim Umgang mit Informationen und IT-Geräten (z.B. Laptops oder Smartphones) einzuhalten sind. Dienstleister und Lieferanten sind definiert als jene Dritten, die Leistungen auf Basis vertraglicher Beziehungen erbringen.

2. Geltungsbereich

Diese Richtlinie und alle damit verbundenen Regelungen gelten für folgende Unternehmen und Ihre Standorte:

A. Kayser Automotive Systems GmbH, Einbeck
A. Kayser Automotive Systems GmbH u. Co.KG, Glauchau
A. Kayser Automotive Systems Polska Spolka z o.o., Poznan
Kayser Automotive Systems Klodzko Sp. z o.o.
A. Kayser Automotive Ibérica, S.L. Automoción S. Com., Pamplona
Kayser Automotive Systems S en C., Puebla
Kayser Automotive Hungária Kft, Komárom
Kayser Automotive Systems (Changchun) Co., Ltd.
Kayser Automotive Systems USA, LP, Fulton
Kayser Automotive Systems Bulgaria EOOD, Pleven

3. Allgemeine Regelungen

Die Nutzung von Daten oder Software des Auftraggebers auf IT-Systemen oder Speichermedien, die weder vom Auftraggeber noch vom Auftragnehmer zur Verfügung gestellt oder freigegeben wurden, ist unzulässig.

Die Nutzung von Daten oder Software des Auftraggebers auf nicht freigegebenen Speichermedien (z.B. vom Auftraggeber nicht freigegebene Fileservices oder Internet-Cloud-Dienste) ist unzulässig.

Die Weitergabe von Daten an Dritte ist nur mit schriftlicher Zustimmung des Dateneigentümers auf Seiten des Auftraggebers zulässig.

Bevor dem Auftragnehmer Zugang zu vertraulichen oder geheimen Informationen gewährt wird, ist eine schriftliche Regelung über die erforderliche Geheimhaltung zu treffen. Mitarbeiter des Auftragnehmers sind von ihrer Geschäftsleitung zur Geheimhaltung im Sinne der zwischen Auftraggeber und Auftragnehmer bestehenden Geheimhaltungsvereinbarung zu verpflichten. Dem Auftraggeber ist auf Verlangen jederzeit Einsicht in diese Vereinbarungen zu gewähren.

1. Introduction

This document defines the security requirements that service providers and suppliers must comply with when handling information and IT devices (e.g. laptops or smartphones). Service providers and suppliers are defined as those third parties who provide services on the basis of contractual relationships.

2. Scope of application

This policy and all associated regulations apply to the following companies and their locations:

A. Kayser Automotive Systems GmbH, Einbeck
A. Kayser Automotive Systems GmbH u. Co.KG, Glauchau
A. Kayser Automotive Systems Polska Spolka z o.o., Poznan
Kayser Automotive Systems Klodzko Sp. z o.o.
A. Kayser Automotive Ibérica, S.L. Automoción S. Com., Pamplona
Kayser Automotive Systems S en C., Puebla
Kayser Automotive Hungária Kft, Komárom
Kayser Automotive Systems (Changchun) Co., Ltd.
Kayser Automotive Systems USA, LP, Fulton
Kayser Automotive Systems Bulgaria EOOD, Pleven

3. General regulations

The use of the Client's data or software on IT systems or storage media that have not been provided or approved by either the Client or the Contractor is not permitted.

The use of the client's data or software on non-approved storage media (e.g. file services or Internet cloud services not approved by the client) is not permitted.

The disclosure of data to third parties is only permitted with the written consent of the data owner on the part of the client.

Before the Contractor is granted access to confidential or secret information, a written agreement on the necessary confidentiality must be concluded. The Contractor's employees shall be obliged by their management to maintain confidentiality in accordance with the confidentiality agreement between the Client and the Contractor. The Client shall be granted access to these agreements at any time upon request.

Soweit Daten des Auftraggebers auf mobilen Systemen oder IT-Geräten gespeichert werden, sind diese mit einer dem Stand der Technik entsprechenden Hard- oder Software zu verschlüsseln (Festplattenverschlüsselung).

Nach Vertragsende sind die Daten des Auftraggebers dem Auftraggeber zu übergeben und auf den Geräten und Speichermedien des Auftragnehmers zu löschen. Gesetzliche Vorgaben (z.B. Aufbewahrungspflichten) sind zu beachten.

Zwischen Auftragnehmer und Auftraggeber ist ein Eskalationsprozess für den Umgang mit Verstößen gegen Vereinbarungen und Sicherheitsanforderungen zu vereinbaren.

3.1. Personalsicherheit

Alle im Namen des Auftragnehmers handelnden Personen, die einen lokalen oder Fernzugriff auf die Informationssysteme des Auftraggebers benötigen, müssen Angaben zu ihrer Identität machen. Der Auftragnehmer stellt sicher, dass der Zugang in seinem Namen nicht missbraucht wird, und übernimmt die volle Verantwortung, falls dies doch geschieht.

Nicht mehr benötigte Benutzerkennungen oder Zugriffsberechtigungen auf Daten des Auftraggebers sind vom jeweiligen Nutzer unverzüglich der auftraggebenden Stelle (z.B. dem zuständigen Benutzeradministrator des Auftraggebers) mitzuteilen, damit eine entsprechende Sperrung/Löschung erfolgen kann.Nicht mehr benötigte Identifikationsmedien (z.B. Smartcards) sind unverzüglich an die auftraggebende Stelle zurückzugeben.

Überlassene Geräte (z.B. Laptops) und Datenträger bzw. Speichermedien sind nach Beendigung des Vertrages oder bei Wegfall der Notwendigkeit an den Auftraggeber zurückzugeben.Der Verlust von dem Nutzer überlassenen IT-Geräten und Authentifizierungsmedien ist vom Nutzer unverzüglich der zuständigen Stelle des Auftraggebers zu melden.

3.2. Physische und umgebungsbezogene Sicherheit

Datenverarbeitungsanlagen, die Daten des Auftraggebers speichern oder verarbeiten, sind so zu betreiben, dass Unbefugte diese Daten nicht einsehen oder darauf zugreifen können. Besondere Vorsicht ist bei der Verwendung mobiler Systeme geboten.
Vertrauliche und geheime Unterlagen dürfen niemals unbeaufsichtigt gelassen werden, um eine Einsichtnahme durch Unbefugte zu verhindern.

If the client's data is stored on mobile systems or IT devices, these must be encrypted using state-of-the-art hardware or software (hard disk encryption).

After the end of the contract, the client's data must be handed over to the client and deleted from the contractor's devices and storage media. Legal requirements (e.g. retention obligations) must be observed.

An escalation process for dealing with breaches of agreements and safety requirements must be agreed between the contractor and the client.

3.1. Personnel security

All persons acting on behalf of the Contractor who require local or remote access to the Client's information systems must provide details of their identity. The Contractor shall ensure that access in its name is not misused and shall assume full responsibility if this does occur.

User IDs or access authorizations to the client's data that are no longer required must be reported immediately by the respective user to the ordering party (e.g. the client's responsible user administrator) so that they can be blocked/deleted accordingly.
Identification media that are no longer required (e.g. smartcards) must be returned to the ordering party immediately.

Equipment provided (e.g. laptops) and data carriers or storage media must be returned to the client upon termination of the contract or when no longer required.
The loss of IT devices and authentication media provided to the user must be reported immediately by the user to the responsible office of the client.

3.2. Physical and environmental safety

Data processing systems that store or process the client's data must be operated in such a way that unauthorized persons cannot view or access this data. Particular care must be taken when using mobile systems.
Confidential and secret documents must never be left unattended in order to prevent unauthorized access.

3.3. Management von organisationseigenen Assets

3.3.1.Klassifizierung

Die Informationen sind auf der Grundlage der rechtlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit in Bezug auf eine unbefugte Offenlegung oder Änderung zu klassifizieren. Gegebenenfalls ist die Klassifizierung auf die Werte für die Speicherung, Verarbeitung oder Handhabung von klassifizierten Informationen auszudehnen.

3.3.1.1. Vertraulichkeit

Für die Einstufung von Informationen hinsichtlich der Anforderungen an die Vertraulichkeit werden folgende Stufen festgelegt:

Öffentlich
Daten sind für jedermann, auch außerhalb der Firma, zugänglich.

Intern
Informationen, die ausschließlich für den internen Gebrauch bestimmt sind und niemals öffentlich werden dürfen. Dies sind insbesondere Informationen, die jedem Mitarbeiter von Kayser Automotive verfügbar sind.

Vertraulich
Vertraulich definierte Daten sind lediglich einer begrenzten Anzahl an Mitarbeitern zugänglich, z.B. Personaldaten, Kundenlisten, Kalkulationen.

Streng vertraulich
Streng Vertrauliche Daten sind punktuell und ausschließlich bestimmten definierten Personen zugänglich. Eine Weitergabe kann das Unternehmen nachhaltig schädigen.

3.3.1.2. Integrität

Es werden die folgenden Stufen verwendet, um die Integrität zu klassifizieren:

Gering
Wenn die Integrität nicht gewährleistet werden kann, sind die Auswirkungen gering.

Mittel
Wenn die Integrität nicht gewährleistet werden kann, sind mäßige Auswirkungen wahrscheinlich.

3.3. Management of the organization's own assets

3.3.1.Classification

Information shall be classified based on legal requirements, its value, criticality and sensitivity to unauthorized disclosure or modification. Where appropriate, the classification shall be extended to the values for the storage, processing or handling of classified information.

3.3.1.1. Confidentiality

The following levels are defined for the classification of information with regard to confidentiality requirements:

Public
Data is accessible to everyone, even outside the company.

Internal
Information that is intended exclusively for internal use and must never become public. In particular, this is information that is available to every employee of Kayser Automotive.

Confidential
Confidentially defined data is only accessible to a limited number of employees, e.g. personnel data, customer lists, calculations.

Strictly confidential
Strictly confidential data is only accessible to certain defined persons on a selective basis. Disclosure can cause lasting damage to the company.

3.3.1.2. Integrity

The following levels are used to classify integrity:

Low
If integrity cannot be guaranteed, the impact is minimal.

Medium
If integrity cannot be guaranteed, moderate effects are likely.

Hoch Bei Verletzung der Integrität sind schwerwiegende, kurzfristige Auswirkungen zu erwarten. Reputation oder taktische Ziele werden beeinträchtigt.	High Serious, short-term consequences are to be expected if integrity is breached. Reputation or tactical objectives are impaired.
Sehr hoch Schwerwiegende Auswirkungen auf langfristige strategische Ziele, die die gesamte Geschäftstätigkeit des Unternehmens stark gefährden.	Very high Serious impact on long-term strategic goals, severely jeopardizing the company's overall business activities.
3.3.1.3. Verfügbarkeit Informationen müssen innerhalb eines vereinbarten Zeitraums verfügbar sein. Zu diesem Zweck werden die folgenden Stufen für die Klassifizierung von Informationen hinsichtlich der Anforderungen an die Verfügbarkeit festgelegt:	**3.3.1.3. Availability** Information must be available within an agreed period of time. For this purpose, the following levels are defined for the classification of information with regard to availability requirements:
Gering Es besteht ein geringes Risiko eines finanziellen Verlustes aufgrund der Ausfallzeit. RTO (Recovery Time Objective) ist größer als eine Woche	Low There is a low risk of financial loss due to downtime. RTO (Recovery Time Objective) is greater than one week
Mittel Es besteht ein mittleres Risiko eines finanziellen Verlustes. Die RTO ist größer als ein Tag und kann zu einem Imageschaden in der Öffentlichkeit führen.	Medium There is a medium risk of financial loss. The RTO is greater than one day and can lead to damage to the company's public image.
Hoch Es besteht ein hohes Risiko eines finanziellen Verlustes. Die RTO ist länger als eine Stunde und kann zu Unannehmlichkeiten für den Kunden und zu einem Imageschaden führen.	High There is a high risk of financial loss. The RTO is longer than one hour and can lead to inconvenience for the customer and damage to the company's image.
Sehr hoch Es besteht das Risiko eines sehr hohen finanziellen Schadens. Der RTO ist größer als eine Stunde und wird die Kundenbeziehung nachhaltig belasten und unter Umständen zum Verlust des Kunden führen. Der Imageverlust in der Öffentlichkeit ist erheblich. Der Schaden ist existenzbedrohend.	Very high There is a risk of very high financial damage. The RTO is greater than one hour and will have a lasting negative impact on the customer relationship and may lead to the loss of the customer. The loss of public image is considerable. The damage is life-threatening.
3.3.2.Kennzeichnung Informationen sind entsprechend ihrer Kritikalität zu kennzeichnen.	**3.3.2.Labeling** Information must be labeled according to its criticality.
Öffentlich Keine Kennzeichnung erforderlich.	Public No labeling required.
Intern Kennzeichnung als „Intern“.	Internal Marking as "Internal".

Vertraulich
Kennzeichnung als „Vertraulich“ in elektronischer oder gedruckter Form.

Streng vertraulich
Kennzeichnung als „Streng vertraulich“ in elektronischer oder gedruckter Form.

3.3.3.Umgang mit Informationen und Datenträgern

Für Informationen der verschiedenen Geheimhaltungsgrade gelten unterschiedliche Anforderungen an die Reproduktion, Speicherung, Löschung und Entsorgung.

Öffentlich
Öffentliche Informationen unterliegen keinen Beschränkungen hinsichtlich Vervielfältigung, Verbreitung, Speicherung, Löschung und Entsorgung.

Intern
Interne Informationen dürfen nur an Mitarbeiter und befugte Nutzer innerhalb ihres Aufgaben- oder Anwendungsbereiches weitergegeben werden. Bei der Speicherung sind die Informationen vor unbefugter Einsichtnahme zu schützen. Die vorhandenen Löschfunktionen sind zu nutzen und die Informationen sind ordnungsgemäß zu entsorgen (DIN 66399 Klasse 3).

Vertraulich
Vertrauliche Informationen dürfen nur an einen begrenzten Verteilerkreis autorisierter Nutzer innerhalb des Aufgaben- bzw. Anwendungsbereichs weitergegeben werden. Dabei sind geeignete Verteilungswege zu nutzen. Die elektronische Übermittlung hat verschlüsselt zu erfolgen. Die Speicherung erfolgt in verschlüsselter Form an geeigneten Speicherorten, die nur den Nutzern im Aufgaben- oder Anwendungsbereich zugänglich sind. Die Löschung erfolgt unwiederbringlich, die Entsorgung / Vernichtung von Informationsträger erfolgt gemäß den Vorgaben der ISO/IEC 21964-2 mit der Sicherheitsstufe 4. Sollte es sich bei den Daten um personenbezogene Daten im Sinne der DSGVO handeln so hat die Vernichtung gemäß den Vorgaben der ISO/IEC 21964-2 mit der Sicherheitsstufe 5.

Streng vertraulich
Streng vertrauliche Informationen dürfen nur an einen eng begrenzten Verteilerkreis autorisierter Nutzer innerhalb des Aufgaben- oder Anwendungsbereiches weitergegeben werden. Die Genehmigung des Informationseigentümers ist erforderlich. Es sind geeignete Verteilungswege zu verwenden. Die elektronische Übermittlung hat verschlüsselt zu erfolgen. Die Speicherung erfolgt an geeigneten Speicherorten, die nur

Confidential
Marking as "Confidential" in electronic or printed form.

Strictly confidential
Marking as "strictly confidential" in electronic or printed form.

3.3.3.Dealing with information and data carriers

Different requirements apply to the reproduction, storage, deletion and disposal of information with different classification levels.

Public
Public information is not subject to any restrictions regarding reproduction, distribution, storage, deletion and disposal.

Internal
Internal information may only be passed on to employees and authorized users within their area of responsibility or application. When storing information, it must be protected against unauthorized access. The existing deletion functions must be used and the information must be disposed of properly (DIN 66399 Class 3).

Confidential
Confidential information may only be passed on to a limited group of authorized users within the scope of the task or application. Suitable distribution channels must be used. Electronic transmission must be encrypted. Storage shall take place in encrypted form at suitable storage locations that are only accessible to users in the task or application area. The deletion is irretrievable, the disposal / destruction of information carriers is carried out in accordance with the specifications of ISO/IEC 21964-2 with security level 4. If the data is personal data within the meaning of the GDPR, it must be destroyed in accordance with the specifications of ISO/IEC 21964-2 with security level 5.

Strictly confidential
Strictly confidential information may only be passed on to a strictly limited group of authorized users within the scope of the task or application. The approval of the information owner is required. Suitable distribution channels must be used. Electronic transmission must be encrypted. Storage shall take place at suitable storage locations that are only accessible in encrypted form to the users in the task or application area. The

den Nutzern im Aufgaben- oder Anwendungsbereich in verschlüsselter Form zugänglich sind. Die Löschung erfolgt unwiederbringlich, die Entsorgung / Vernichtung von Informationsträger erfolgt gemäß den Vorgaben der ISO/IEC 21964-2 mit der Sicherheitsstufe 4. Sollte es sich bei den Daten um personenbezogene Daten im Sinne der DSGVO handeln so hat die Vernichtung gemäß den Vorgaben der ISO/IEC 21964-2 mit der Sicherheitsstufe 5.	deletion is irretrievable, the disposal / destruction of information carriers is carried out in accordance with the specifications of ISO/IEC 21964-2 with security level 4. If the data is personal data within the meaning of the GDPR, the destruction must be carried out in accordance with the specifications of ISO/IEC 21964-2 with security level 5.
Für die Weitergabe von vertraulichen oder geheimen Informationen an Dritte ist eine schriftliche Geheimhaltungserklärung zwingend erforderlich.	A written confidentiality agreement is mandatory for the disclosure of confidential or secret information to third parties.
Datenträger (z. B. CDs, DVDs, USB-Sticks und Festplatten) sind vor Verlust, Zerstörung, Verwechslung und unbefugtem Zugriff zu schützen. Nicht mehr benötigte Datenträger sind sicher zu entsorgen / zu vernichten. Die oben genannten Anforderungen gelten entsprechend.	Data carriers (e.g. CDs, DVDs, USB sticks and hard drives) must be protected against loss, destruction, confusion and unauthorized access. Data carriers that are no longer required must be disposed of / destroyed securely. The above requirements apply accordingly.
3.3.4.Informationsaustausch Bei allen Gesprächen (einschließlich Telefongesprächen, Video- und Webkonferenzen), die vertrauliche oder geheime Informationen betreffen oder enthalten, ist sicherzustellen, dass sie nicht von Unbefugten abgehört werden können. Faxnummern und E-Mail-Adressen sind aktuellen Verzeichnissen zu entnehmen oder beim Empfänger zu erfragen, um Fehlleitungen zu vermeiden. Die Verantwortung für den Inhalt und die Verteilung einer E-Mail liegt beim Absender. Für die weitere Verarbeitung und Verteilung ist der Empfänger verantwortlich.	**3.3.4.Exchange of information** For all conversations (including telephone conversations, video and web conferences) that concern or contain confidential or secret information, it must be ensured that they cannot be intercepted by unauthorized persons. Fax numbers and e-mail addresses should be taken from current directories or requested from the recipient in order to avoid misdirection. The sender is responsible for the content and distribution of an e-mail. The recipient is responsible for further processing and distribution.
3.3.5.Schutz und Ausfallsicherheit Es müssen Mechanismen eingerichtet werden, um die Genauigkeit und Vollständigkeit und somit die Integrität der Informationen während der Verarbeitung zu gewährleisten. Der Auftragnehmer verpflichtet sich, die Verfügbarkeit der Informationen durch Wiederherstellungs- und Notfallverfahren zu gewährleisten. Die gesetzlichen und behördlichen Anforderungen an den Datenschutz und die Regelung von Eigentums- und Urheberrechten sind einzuhalten.	**3.3.5.Protection and reliability** Mechanisms must be put in place to ensure the accuracy and completeness and thus the integrity of the information during processing. The Contractor undertakes to ensure the availability of the information by means of recovery and emergency procedures. The legal and official requirements for data protection and the regulation of property rights and copyrights must be complied with.
3.4. Incident- und Schwachstellenmanagement Der Auftragnehmer ist verpflichtet, dem Auftraggeber unverzüglich Informationssicherheitsereignisse und -vorfälle in seinem Unternehmen zu melden, die potenziell negative Auswirkungen auf die Vermögenswerte des Auftraggebers haben können (z.B. Sicherheitslücken im Quellcode) oder die die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Informationen beeinträchtigen.	**3.4. Incident and vulnerability management** The Contractor is obliged to notify the Client immediately of information security events and incidents in its company that could potentially have a negative impact on the Client's assets (e.g. security vulnerabilities in the source code) or that affect the confidentiality, integrity and/or availability of information.

Im Falle eines Sicherheitsvorfalls stellt der Auftragnehmer auf Anforderung des Auftraggebers Ressourcen zur Minderung und/oder Beseitigung sowie den abschließenden Korrekturbericht zur Verfügung.

Der Auftragnehmer hat seine Produkte regelmäßig auf Schwachstellen zu überprüfen und auf Schwachstellen schnellstmöglich zu reagieren. Sind vom Auftragnehmer entwickelte und/oder gelieferte Soft- oder Hardwarekomponenten von Schwachstellen betroffen, ist der Auftragnehmer verpflichtet, diese unverzüglich dem Auftraggeber zu melden. Die Schwachstellen sind hinsichtlich ihrer sicherheitstechnischen Auswirkungen zu analysieren. Der Umfang der Analyse umfasst jede potenzielle Schwachstelle, die sich auf die Vertraulichkeit, Integrität und/oder Verfügbarkeit der (materiellen oder immateriellen) Vermögenswerte des Auftraggebers auswirken kann.

Der Auftraggeber erkennt an, dass Informationen über die umgebende Infrastruktur oder andere einflussnehmende Umstände nicht vollständig sein können und dass das bestmögliche Ergebnis auf dem Wissen im Branchenumfeld des Auftragnehmers beruht. Zwischen Auftraggeber und Auftragnehmer sind Kriterien für die Meldung und Behebung von Schwachstellen zu vereinbaren. Art und Form der Kommunikation sind zwischen Auftraggeber und Auftragnehmer zu vereinbaren. Für die Übertragung sind Techniken zu verwenden, die die Integrität und Vertraulichkeit der Informationen gewährleisten.

3.5. Patch Management

Der Patch-Umfang muss das gesamte vom Auftraggeber akzeptierte System umfassen.
Der Auftragnehmer stellt sicher, dass alle Systeme vor der Abnahme entsprechend gepatcht und aktualisiert sind. Der Patchstand muss so aktuell wie möglich sein, darf jedoch nicht älter als 6 Monate ab dem Datum der Systemabnahmeerklärung sein. Der Auftragnehmer hat alle öffentlich verfügbaren und vom Auftraggeber freigegebenen Patches als Teil der Lieferung zu installieren.

Der Auftragnehmer verpflichtet sich, bei Bedarf Updates und Patches zur Verfügung zu stellen. Der Auftragnehmer erstellt für jede im Patchzyklus adressierte Schwachstelle einen Bericht und stellt diesen dem Auftraggeber zur Verfügung.
Sollte der Drittanbieter einer Komponente (Betriebssystem, Software etc.) das Ende des Lebenszyklus ankündigen, muss der Auftragnehmer entweder eine aktualisierte Version der Komponente anbieten, eine adäquate Alternative einsetzen oder den weiteren Support für die Bereitstellung von Sicherheitspatches für die ältere Version vertraglich mit dem Drittanbieter sicherstellen.

In Fällen, in denen der Auftragnehmer Anwendungen und/oder andere Funktionalitäten liefert und der Auftraggeber oder andere Drittanbieter in seinem Namen für das Update-

In the event of a security incident, the Contractor shall provide mitigation and/or remediation resources and the final corrective action report at the Client's request.

The Contractor shall regularly check its products for vulnerabilities and respond to vulnerabilities as quickly as possible. If software or hardware components developed and/or supplied by the Contractor are affected by vulnerabilities, the Contractor shall be obliged to report these to the Client without delay. The vulnerabilities shall be analyzed in terms of their security implications. The scope of the analysis shall include any potential vulnerability that may affect the confidentiality, integrity and/or availability of the client's (tangible or intangible) assets.

The Client acknowledges that information about the surrounding infrastructure or other influencing circumstances may not be complete and that the best possible result is based on the knowledge of the Contractor's industry environment. Criteria for reporting and rectifying weaknesses must be agreed between the client and the contractor. The type and form of communication must be agreed between the client and the contractor. Techniques that guarantee the integrity and confidentiality of the information must be used for the transmission.

3.5. Patch Management

The scope of the patch must include the entire system accepted by the client.
The Contractor shall ensure that all systems are patched and updated accordingly prior to acceptance. The patch status must be as up-to-date as possible, but may not be older than 6 months from the date of the system acceptance declaration. The Contractor shall install all publicly available patches approved by the Client as part of the delivery.

The Contractor undertakes to provide updates and patches as required. The Contractor shall prepare a report for each vulnerability addressed in the patch cycle and make it available to the Client.
If the third-party provider of a component (operating system, software, etc.) announces the end of its life cycle, the Contractor must either offer an updated version of the component, use an adequate alternative or ensure continued support for the provision of security patches for the older version by contract with the third-party provider.

In cases where the Contractor delivers applications and/or other functionalities and the Client or other third-party providers on its behalf are responsible for the update

Management der darunter liegenden Schichten, wie z.B. des Betriebssystems, verantwortlich sind, muss der Auftragnehmer die kontinuierliche Funktionsfähigkeit seiner gelieferten Leistung auch bei Patches der darunter liegenden Systemplattform sicherstellen.	management of the underlying layers, such as the operating system, the Contractor must ensure the continuous functionality of its delivered service even in the event of patches to the underlying system platform.
3.6. Systemhärtung Der Auftragnehmer verpflichtet sich, die von ihm gelieferten Assets (z.B. Systeme) angemessen zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren. Dies muss geschehen sein, bevor der Auftraggeber die Abnahme des Systems erklärt.	**3.6. System hardening** The Contractor undertakes to harden the assets it supplies (e.g. systems) appropriately in order to minimize the impact of potential security risks. This must be done before the client declares acceptance of the system.
Jeder nicht benötigte Netzwerkdienst oder -zugang muss deaktiviert werden. Die Verwendung jedes Dienstes oder Zugangs ist in der Dokumentation des Auftragnehmers zu erläutern.	Any network service or access that is not required must be deactivated. The use of each service or access must be explained in the Contractor's documentation.
Der Auftragnehmer stellt sicher, dass die vom Auftraggeber vorgegebenen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden. Der Auftragnehmer stellt sicher, dass jedes Standardpasswort in allen möglichen Fällen geändert werden kann.	The Contractor shall ensure that the configuration standards and safety regulations specified by the Client are complied with. The Contractor shall ensure that each standard password can be changed in all possible cases.
Der Auftragnehmer stellt im Rahmen seiner Möglichkeiten sicher, dass seine Produkte frei von „Hintertüren“ sind, mit denen die verwendeten Sicherheitsmechanismen umgangen werden können.Der Auftragnehmer verpflichtet sich, für seine Produkte durch geeignete Maßnahmen und Protokolle, die mit dem Auftraggeber abzustimmen sind, nachzuweisen, dass alle im Abschnitt „Systemhärtung“ genannten Anforderungen eingehalten werden.	As far as possible, the contractor shall ensure that its products are free of "back doors" with which the security mechanisms used can be circumvented.The Contractor undertakes to prove that all requirements specified in the section "System hardening" are met for its products by means of suitable measures and protocols to be agreed with the Client.
3.7. Fernzugang für Drittanbieter Der Auftragnehmer muss sicherstellen, dass bei Fernzugriffen die Vertraulichkeit, Integrität und Verfügbarkeit der Einrichtungen und Dienste des Auftraggebers gewährleistet ist. Dies schließt die Weiterverwendung von Informationen ein, von denen der Auftragnehmer, während eines Fernzugriffs Kenntnis erlangt hat. Er ist für alle Aktionen der ihm zugewiesenen Benutzerkonten mit Fernzugriffsfunktion auf den Systemen des Auftraggebers verantwortlich.	**3.7. Remote access for third-party providers** The Contractor must ensure that the confidentiality, integrity and availability of the Client's facilities and services are guaranteed during remote access. This includes the further use of information of which the Contractor has gained knowledge during remote access. He is responsible for all actions of the user accounts assigned to him with remote access function on the client's systems.
Zum Zwecke der Nachvollziehbarkeit erhält jeder Benutzer auf Seiten des Auftragnehmers ein eigenes Benutzerkonto. Ausnahmen sind gesondert zu vereinbaren und zu dokumentieren. In diesem Fall stellt der Auftragnehmer die Nachvollziehbarkeit der Nutzung des Benutzerkontos (wer und wann) sicher und übergibt dem Auftraggeber auf Anforderung die Dokumentation. Sollte der Auftragnehmer ein Benutzerkonto nicht mehr benötigen, ist der Auftraggeber unverzüglich zu informieren, damit das Benutzerkonto	For the purpose of traceability, each user shall receive a separate user account on the part of the Contractor. Exceptions must be agreed and documented separately. In this case, the Contractor shall ensure the traceability of the use of the user account (who and when) and hand over the documentation to the Client on request. If the Contractor no longer requires a user account, the Client must be informed immediately so that the user

gesperrt werden kann. Die Authentifizierungsverfahren sind zwischen Auftragnehmer und Auftraggeber zu vereinbaren.

3.8. Anforderungen an die Softwareentwicklungsprozesse

Die Softwareentwicklungsprozesse des Auftragnehmers müssen so gestaltet sein, dass die Sicherheit der entwickelten Software in allen Entwicklungsphasen gewährleistet ist.

3.9. Kryptographie

Die zulässigen kryptographischen Verfahren und die Mindestlängen der kryptographischen Schlüssel sind zwischen Auftraggeber und Auftragnehmer festzulegen. Es sind nur Verfahren zulässig, die nach dem Stand der Technik als sicher gelten. Dabei ist auf bestehende Industriestandards (z.B. BSI TR-02102) zurückzugreifen. Verfahren und Schlüssellängen, die nicht den Anforderungen entsprechen, gelten entsprechend als Schwachstellen (siehe Abschnitt „Schwachstellenmanagement“). Der Auftragnehmer muss sicherstellen, dass die kryptografische Absicherung der Kommunikation und Speicherung überall dort erfolgt, wo es zur Unterstützung der Prinzipien der sicheren Softwarearchitektur erforderlich ist.

3.10. Dokumentation

Der Auftragnehmer stellt dem Auftraggeber die für den Betrieb der von ihm gelieferten Anlagen erforderliche Dokumentation zur Verfügung. Der Umfang der Dokumentation muss mindestens die folgenden Punkte umfassen:

- Liste der Hardware
- Liste der Software (inkl. Betriebssystem und Patch-Level)
- Übersicht über die Systemarchitektur
- Kommunikationsmatrix
- vorhandene Benutzerkonten und Rollen sowie deren Berechtigungen
- ausreichende Beschreibung proprietärer (nicht industrieüblicher) Sicherheitsmechanismen
- weitere Dokumentationen, die als Teil des Liefergegenstandes oder des Auftrages spezifiziert sind und die Sicherheit des Produktes gewährleisten.

Werden Änderungen am Liefergegenstand vorgenommen, so hat der Auftragnehmer die Dokumentation entsprechend anzupassen.

3.11. Nicht-technische Sicherheit

Der Auftragnehmer kommt der Aufforderung des Auftraggebers nach, Informationen über seine Sicherheitsorganisation offen zu legen, auf deren Grundlage der Auftraggeber eine Bewertung des Auftragnehmers vornehmen kann. Der Auftragnehmer muss alle

account can be blocked. The authentication procedures must be agreed between the contractor and the client.

3.8. Requirements for the software development processes

The contractor's software development processes must be designed in such a way that the security of the developed software is guaranteed in all development phases.

3.9. Cryptography

The permitted cryptographic procedures and the minimum lengths of the cryptographic keys must be agreed between the client and the contractor. Only procedures that are considered secure according to the state of the art are permitted. Existing industry standards (e.g. BSI TR-02102) must be used. Procedures and key lengths that do not meet the requirements are considered vulnerabilities accordingly (see section "Vulnerability management"). The Contractor must ensure that cryptographic protection of communication and storage is provided wherever necessary to support the principles of secure software architecture.

3.10. Documentation

The Contractor shall provide the Client with the documentation required for the operation of the systems supplied by it. The scope of the documentation must include at least the following points:

- List of hardware
- List of software (incl. operating system and patch level)
- Overview of the system architecture
- Communication matrix
- Existing user accounts and roles and their authorizations
- Sufficient description of proprietary (non-industry standard) security mechanisms
- other documentation that is specified as part of the delivery item or the order and ensures the safety of the product.

If changes are made to the delivery item, the Contractor shall adapt the documentation accordingly.

3.11. Non-technical security

The Contractor shall comply with the Client's request to disclose information about its security organization, on the basis of which the Client can make an assessment of the Contractor.The Contractor must identify and document all resources in its information

Ressourcen in seinen Informationssystemen identifizieren und dokumentieren, die einen Bezug zu den Informationssystemen des Auftraggebers für die Wartung oder den operativen Zugang haben können. Die Verantwortung für die Aufrechterhaltung der erforderlichen Sicherheitskontrollen für diese Anlagen muss zugewiesen werden.	systems that may have a connection to the Client's information systems for maintenance or operational access. Responsibility for maintaining the required security controls for these assets must be assigned.
Der Auftragnehmer kann die Anwendung spezifischer Sicherheitsmaßnahmen zum Schutz der Werte delegieren, bleibt jedoch für den angemessenen Schutz der Werte, die mit den Informationssystemen des Auftraggebers in Verbindung stehen, verantwortlich. Wenn der Auftragnehmer zur Erfüllung des Vertrags mit dem Auftraggeber mit Unterauftragnehmern zusammenarbeitet, muss er sicherstellen, dass der Unterauftragnehmer dieselben Anforderungen erfüllt.	The Contractor may delegate the application of specific security measures to protect the assets, but remains responsible for the adequate protection of the assets associated with the Client's information systems. If the contractor works with subcontractors to fulfill the contract with the client, he must ensure that the subcontractor meets the same requirements.
Soweit der Auftragnehmer Unterauftragnehmer mit der Erbringung von Leistungen oder Teilen von Leistungen beauftragt, hat er diese ausdrücklich als Unterauftragnehmer zu kennzeichnen und ist verpflichtet, dafür Sorge zu tragen, dass die mit ihm vereinbarten Sicherheitsanforderungen vom Unterauftragnehmer in angemessenem Umfang eingehalten werden. Der Auftragnehmer ist für die Überwachung der Einhaltung der Sicherheitsanforderungen durch seine Unterauftragnehmer und für die Einhaltung der weitergegebenen Anforderungen verantwortlich.	If the Contractor commissions subcontractors with the provision of services or parts of services, it must expressly identify them as subcontractors and is obliged to ensure that the safety requirements agreed with it are complied with by the subcontractor to an appropriate extent. The Contractor shall be responsible for monitoring compliance with the safety requirements by its subcontractors and for compliance with the requirements passed on.
Auf Verlangen des Auftraggebers ist der Auftragnehmer verpflichtet, für den Umgang mit sensibler Ausrüstung sowohl vor der Integration in das Netz des Auftraggebers als auch für die Wartung der sensiblen Ausrüstung während der gesamten Betriebsphase nur geprüftes, z.B. von nationalen Behörden geprüftes Sicherheitspersonal einzusetzen. Relevante Informationen (insbesondere die Identifizierung und Bestimmung der sensiblen Ausrüstung) müssen schriftlich vereinbart werden. Ausnahmeregelungen der lokalen Gesetzgebung sind zu beachten.	At the Client's request, the Contractor is obliged to use only security personnel who have been tested, e.g. by national authorities, for handling sensitive equipment both before integration into the Client's network and for maintaining the sensitive equipment during the entire operating phase. Relevant information (in particular the identification and destination of the sensitive equipment) must be agreed in writing. Exceptions to local legislation must be observed.
Der Auftragnehmer setzt nur Personen ein, die über entsprechende Kenntnisse und Fähigkeiten in Bezug auf Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung(en) verfügen.	The Contractor shall only deploy persons who have the appropriate knowledge and skills with regard to installation, software or hardware, maintenance or operation of the solution(s).
3.12. Auditierung Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder ein von ihm beauftragter Dritter im Namen des Auftraggebers Audits in Bezug auf die Informationssicherheit des Auftragnehmers durchführen kann. Die Audits werden auf der Grundlage der vom Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden einvernehmlich festgelegt. Darüber hinaus hat der Auftragnehmer Abweichungen von den vereinbarten Sicherheitsanforderungen anzuzeigen.	**3.12. Auditing** The Contractor agrees that the Client or a third party commissioned by the Client may carry out audits on behalf of the Client with regard to the Contractor's information security. The audits shall be carried out on the basis of the documentation provided by the Contractor. The exact scope, duration and organization shall be determined by mutual agreement. In addition, the Contractor must report any deviations from the agreed safety requirements.

3.13. Verstöße und Durchsetzung Verstöße gegen die Informationssicherheitsanforderungen sind im Einzelfall gemäß den geltenden betrieblichen, vertraglichen und gesetzlichen Regelungen und Vereinbarungen zu untersuchen und zu ahnden.	**3.13. Violations and enforcement** Violations of the information security requirements must be investigated and punished on a case-by-case basis in accordance with the applicable operational, contractual and legal regulations and agreements.

Sicherheitsrichtlinie: Richtlinie für Partnerfirmen

Security Guideline: Guideline for partner companies

Revision	Änderung / Change	Datum / Date	Ersteller / Author	Teilnehmer	Prozessowner / process owner
01	Erstellung / Creation	17.11.2014	F. Mollenhauer		-
02	Dok. Nummer aktualisiert / Update doc. number	01.08.2017	L. Diekmann		
03	Inhaltliche Überarbeitung / Contentual revision	05.06.2018	L. Diekmann		
04	Grundlegende Überarbeitung / General revision	23.04.2024	S. Giske		