Ergänzende Vorgaben für die Lieferung von Informations- und Kommunikationstechnologie-Anteilen in Anlagen und pay-per-use Fertigungsleistungen

Stand per 9.3.2026

Die in diesem Dokument festgelegten Bestimmungen ergänzen die Regelungen des Dokuments „IT-Sicherheit-Mindeststandards für externe Partner".
Soweit einzelne Regelungen dieses Dokuments über die Anforderungen der „IT-Sicherheit-Mindeststandards für externe Partner" hinausgehen oder diesen widersprechen, gehen die Bestimmungen dieses Dokuments vor. Die Verpflichtung zur Einhaltung der „IT-Sicherheit-Mindeststandards für externe Partner" bleibt davon unberührt und ist jedenfalls vollumfänglich einzuhalten.

Der Auftragsverarbeiter/Auftragnehmer (AN) ist verpflichtet, bei der, Planung, Architektur, Umsetzung, dem Betrieb sowie der Wartung sämtlicher von ihm erbrachter Leistungen bzw. gelieferter Produkte aus den Bereichen Informationstechnologie (IT), Operational Technology (OT), Telekommunikation, Automatisierung, Digitalisierung, Software, Hardware, Netzwerk und Sicherheitstechnik sowie aller damit in Zusammenhang stehenden Beratungs- , Support , Service und sonstigen Dienstleistungen gegenüber des Auftraggebers (AG) alle jeweils gültigen gesetzlichen, regulatorischen und normativen Anforderungen vollumfänglich einzuhalten.

1 Einhaltung von Industrienormen

Der AN hat insbesondere sicherzustellen, dass die Anforderungen der NIS2-Richtlinie sowie der Normenreihe IEC 62443 in der jeweils gültigen Fassung verbindlich eingehalten werden. Sicherheitsanforderungen sind zwingend bereits in der Konzeptions- und Designphase (Security by Design und Security by Default) zu berücksichtigen und während des gesamten Lebenszyklus der Leistung wirksam aufrechtzuerhalten. Der AN hat dem AG auf Verlangen unverzüglich geeignete und nachvollziehbare Nachweise über die Einhaltung dieser Anforderungen zur Verfügung zu stellen.

2 Sicheres Design (Security by Design / Security by Default)

Der AN hat sicherzustellen, dass Sicherheitsanforderungen bereits in der Konzeptions- und Designphase der erbrachten Leistung verbindlich berücksichtigt werden.
Dabei sind insbesondere folgende Grundsätze einzuhalten:

- Minimierung der Angriffsfläche
- Trennung von Zonen, Systemen und Funktionen
- Prinzip der minimalen Rechtevergabe („Least Privilege")
- Vermeidung unnötiger Schnittstellen, Dienste und Kommunikationspfade

Die Architektur muss geeignet sein um die Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Systeme und Daten des AG dauerhaft sicherzustellen.

3 Sichere Implementierung

Die Implementierung von Dienstleistungen und Komponenten im Automatisierungsumfeld hat gemäß dem Stand der Technik und unter Berücksichtigung anerkannter sicherer Entwicklungs- und Implementierungspraktiken zu erfolgen.
Insbesondere ist sicherzustellen, dass:

- Standard und Default Konfigurationen überprüft und sicher gehärtet werden
- nicht benötigte Dienste, Benutzerkonten und Schnittstellen deaktiviert sind
- sicherheitsrelevante Konfigurationen dokumentiert und nachvollziehbar umgesetzt werden

Eigenmächtige Änderungen an Systemkonfigurationen oder Sicherheitsmechanismen sind unzulässig und bedürfen der vorherigen Freigabe durch den AG.

voestalpine
ONE STEP AHEAD.

4 Sicherer Betrieb

Der Betrieb der eingesetzten Systeme und Komponenten hat kontrolliert, nachvollziehbar und unter Einhaltung der definierten Sicherheitsvorgaben zu erfolgen.
Der AN hat sicherzustellen, dass:

- Zugriffe auf Systeme und Komponenten protokolliert und nachvollziehbar sind
- sicherheitsrelevante Ereignisse erkannt und gemeldet werden
- Betriebs- und Sicherheitsparameter regelmäßig überprüft werden

Der Betrieb darf keine Umgehung bestehender Sicherheits-, Überwachungs- oder Schutzmechanismen des AG ermöglichen.

5 Wartung und Änderungen

Wartungs-, Update- und Instandhaltungsarbeiten an Systemen und Komponenten im Automatisierungsumfeld dürfen ausschließlich nach vorheriger Abstimmung und Freigabe durch den AG durchgeführt werden.
Dabei ist sicherzustellen, dass:

- Änderungen kontrolliert, dokumentiert und nachvollziehbar erfolgen
- sicherheitsrelevante Updates zeitnah und abgestimmt umgesetzt werden
- die Funktionsfähigkeit und Sicherheit der Systeme nach Wartungsarbeiten überprüft werden

Nicht abgestimmte oder unautorisierte Wartungs- oder Änderungsmaßnahmen sind untersagt.

5.1 Dokumentations- und Übergabepflichten bei Änderungen

Der AN ist verpflichtet, sämtliche Änderungen im Zusammenhang mit Design, Implementierung, Konfiguration, Betrieb oder Wartung von Dienstleistungen, Systemen oder Komponenten im IT und Automatisierungs-/OT Umfeld des AG vollständig, nachvollziehbar und zeitnah zu dokumentieren.

5.2 Dokumentationspflicht

Der AN hat sicherzustellen, dass insbesondere folgende Inhalte dokumentiert werden:

- Beschreibung der durchgeführten Änderung(en)
- betroffene Systeme, Komponenten, Schnittstellen oder Konfigurationen
- Zeitpunkt und Anlass der Änderung
- durchführende Personen bzw. Organisationseinheiten
- Auswirkungen auf Sicherheit, Betrieb und Verfügbarkeit

Die Dokumentation ist in einer Form zu erstellen, die eine fachliche Nachvollziehbarkeit sowie eine Verwendung für Betriebs-, Wartungs- und Audit- Zwecke ermöglicht.

5.3 Übergabe an den Auftraggeber

Änderungs-, Betriebs- und Sicherheitsdokumentationen sind dem AG unverzüglich nach Durchführung der jeweiligen Änderung vollständig zu übergeben.
Die Übergabe hat in einem vom AG akzeptierten Format zu erfolgen und umfasst insbesondere:

- aktualisierte Architektur-, System- oder Netzpläne
- Konfigurations- und Betriebshandbücher
- sicherheitsrelevante Parameter und Einstellungen

Die Verantwortung für die ordnungsgemäße und vollständige Übergabe der Dokumentation liegt ausschließlich beim AN.

5.4 Betriebsrelevanz und Wissenssicherung

Der AN hat sicherzustellen, dass die übergebene Dokumentation den AG in die Lage versetzt, den sicheren Betrieb der Systeme eigenständig sicherzustellen, Wartungs- und Störungsmaßnahmen nachvollziehbar durchführen zu können, sowie regulatorische, normative oder interne Auditanforderungen zu erfüllen. Unvollständige, verspätete oder nicht übergebene Dokumentationen gelten als nicht ordnungsgemäße Leistungserbringung.

voestalpine
ONE STEP AHEAD.

6 Verbot unautorisierter Netzwerkverbindungen

Das eigenmächtige oder unautorisierte Verbinden von Geräten, Systemen oder Komponenten jeglicher Art mit bestehenden Netzwerk-, Kommunikations- oder OT-Strukturen des AG ist strengstens untersagt. Eine Verbindung darf ausschließlich nach vorheriger ausdrücklicher schriftlicher Freigabe durch den AG erfolgen. Verstöße gelten als schwerwiegende Sicherheitsverletzung.

7 Verbot von USB-Speichergeräten

Die Verwendung von USB-Speichergeräten, externen Datenträgern sowie sonstigen Wechselmedien ist grundsätzlich untersagt. Ausnahmen bedürfen einer vorherigen schriftlichen Genehmigung des AG.

8 Verbot von Modems und drahtlosen Übertragungsgeräten

Der Einbau, Betrieb oder Anschluss von Modems, Routern, WLAN-, Mobilfunk- oder sonstigen drahtlosen Übertragungsgeräten jeglicher Art ist untersagt. Abweichungen sind ausschließlich nach schriftlicher Genehmigung des AG zulässig.

9 Verpflichtende Sicherheits-Schulung

Vor Aufnahme jeglicher Tätigkeit im IT-/OT-Umfeld des AG ist sicherzustellen, dass alle eingesetzten Mitarbeiter die IT/OT-spezifische Sicherheits-Schulung erfolgreich absolviert haben. Von Mitarbeitern ohne gültige IT/OT-spezifische Sicherheits-Schulung dürfen keine Tätigkeiten verrichten werden.

10 Remote Access Regelungen

Der Zugriff auf Systeme, Netzwerke oder OT-Umgebungen des AG mittels Fernzugriff (Remote Access) ist ausschließlich unter den nachstehenden Bedingungen zulässig.

10.1 Zulässige Remote Access- -Lösungen

Für den Fernzugriff dürfen ausschließlich jene Remote Access Lösungen verwendet werden, die vom AG ausdrücklich freigegeben wurden.
Die Nutzung nicht genehmigter Remote Access Lösungen, Werkzeuge, Dienste oder Verfahren ist untersagt. Dies gilt insbesondere für eigenständig installierte oder cloudbasierte Fernzugriffslösungen, unabhängig davon, ob diese dauerhaft oder temporär eingesetzt werden.

10.2 Freigabe- und Nutzungsvoraussetzungen

Remote Zugriffe dürfen nur nach vorheriger schriftlicher Freigabe durch den AG und ausschließlich im genehmigten Umfang erfolgen.
Der Remote Access ist auf das für die Leistungserbringung unbedingt erforderliche Mindestmaß zu beschränken („Least Privilege"-Prinzip). Eine dauerhafte oder unbeaufsichtigte Verbindung ist unzulässig, sofern diese nicht ausdrücklich vom AG genehmigt wurde.

10.3 Sicherheitsanforderungen an den Remote Access

Der eingesetzte Remote Access muss dem Stand der Technik entsprechen und insbesondere eine verschlüsselte Kommunikation sowie eine starke Authentifizierung (z. B. Mehr Faktor Authentifizierung) gewährleisten. Der AN hat sicherzustellen, dass über den Remote Access keine Umgehung bestehender Sicherheitsmechanismen, Netzwerksegmentierungen oder Zugriffsbeschränkungen des AG möglich ist.

10.4 Protokollierung und Kontrolle

Remote Access Verbindungen unterliegen der Protokollierung und Überwachung durch den AG. Der AN erkennt ausdrücklich an, dass sämtliche Remote Zugriffe nachvollziehbar aufgezeichnet werden können und auf Verlangen entsprechende Nachweise zur Verfügung zu stellen sind.

voestalpine
ONE STEP AHEAD.

11 Verwendung von voestalpine IT Standardgeräten und Services

Soweit möglich sind Hardware-Komponenten (Computer mit Microsoft, Linux oder iOS Betriebssystemen, Monitore, ...) gemäß voestalpine Standard einzusetzen. Der Bedarf an diesen Geräten ist im Angebot darzustellen, die Geräte werden durch voestalpine beigestellt. Etwaige abweichende Hardware-Anforderungen sind explizit darzustellen und zu begründen.

Sofern Virtualisierung (für Server oder Clients) zum Einsatz kommen soll, sind die erforderlichen virtuellen Maschinen mit ihren Anforderungen (Anzahl Cores, Hauptspeicher- und Festplattenbedarf, ...) zu spezifizieren. Die Virtualisierungsumgebung wird gemäß voestalpine Standard von voestalpine bereitgestellt.

12 Client Konfiguration

Für Windows-Client-Systeme im Produktionsbereich sind die zum Zeitpunkt der Auftragsvergabe aktuellsten und von Microsoft supporteten Betriebssystemversionen zu verwenden.

13 Asset Management

Alle Computersysteme müssen im voestalpine Asset Management dokumentiert werden. Dies erfolgt durch initiales Scannen der Systeme nach vollständiger Installation und anschließendes regelmäßiges Scannen mit der voestalpine Scanner Software. Vom AN ist vor Inbetriebnahme eine vollständige Liste der Computersysteme in seinem Lieferumfang incl. der vom AG auf Anforderung des AN beigestellten Computersysteme bereitzustellen und die Scan-Bereitschaft der Systeme bekanntzugeben.

14 Lizenz-Management

Die Anlagen-IT muss vollständig sein, incl. aller für den Betrieb und den Zugriff auf die Anlage erforderlichen Lizenzen. Der Anbieter hat dafür dem Angebot eine vollständige Auflistung aller erforderlichen Software-Lizenzen sowie jeglicher eingesetzter freier Software (wie z.B. Freeware, Open Source Software, etc.) und alle für die Software geltenden Lizenzbedingungen - inklusive der Zuordnungsinformation, für welche Software(teile) der aufgelisteten welche konkret Lizenzbedingungen jeweils gelten - beizufügen. Der AG behält sich vor, auf ausdrücklichen schriftlichen Wunsch des AG, die Lizenzen für im voestalpine Konzern standardmäßig eingesetzte Software beizustellen. Für im Lieferumfang enthaltene Software sind vom AN neben den soeben genannten Unterlagen und Informationen auch die vollständigen Lizenznachweise an den AG zu übergeben.

15 Netzwerk-Verkabelung

Netzwerkverkabelungen sind gemäß voestalpine Standard auszuführen.

16 Dateneignerschaft und Nutzungsrecht

Jeglicher Zugriff auf Produktionsanlagendaten und Log-Daten durch Externe, insbesondere auch durch den Hersteller der Anlage bzw. Anlagenautomation, erfordert eine ausdrückliche Genehmigung durch voestalpine: Dateneignerschaft und Nutzungsrecht liegen für diese Daten ausschließlich bei voestalpine. Dies umfasst insbesondere auch Daten, welche durch Benutzung des Systems bzw. der Anlage (durch voestalpine) erzeugt werden. Alle durch die Anlage und deren Systeme erzeugten Daten sind und bleiben Eigentum der voestalpine. Jede Art ihrer Nutzung durch Dritte ist schriftlich genehmigungspflichtig und zu dokumentieren; voestalpine prüft die Einhaltung.

17 Internetanbindung

Eine direkte Internetanbindung von Anlagenautomationssystemen und von IP-Netzen/ Segmenten, in denen sich Anlagenautomationssysteme befinden, ist nicht zulässig**.**

18 Zugriff auf Sensordaten

Alle im Lieferumfang des AN anfallenden oder erfassten Sensordaten müssen voestalpine durch ein Standardinterface der Maschinen- oder Anlagenautomation zugänglich gemacht werden. Stehen dem AG geschultes Personal und alle erforderlichen Entwicklungswerkzeuge zur Verfügung, um Schnittstellen der Maschinen- oder Anlagenautomation zu erweitern oder neu zu erstellen, so reicht in Abstimmung mit dem AG die vollständige Dokumentation aller Sensorwerte im Automationssystem.

19 Source Code für Individualsoftware

Für jegliche Individualsoftware (nicht am freien Markt erhältliche Software) der Anlagenautomation sind der Source Code, erforderliche Bibliotheken und die Entwicklungsumgebung zu liefern.

20 Nutzungsdauer

Der Anbieter hat im Angebot darzustellen, wie er den sicheren (auch hinsichtlich IT-Security) Betrieb und die Weiterentwicklungsmöglichkeit der Anlage über mindestens 10 Jahre gewährleisten kann. Aspekte wie Ersatzteilverfügbarkeit, Upgrade von System- und Standardsoftware, Security Patches, … sind dabei zu berücksichtigen. Zum Zeitpunkt der Inbetriebnahme müssen die verwendeten Betriebssysteme und alle Softwarekomponenten auf den aktuellsten verfügbaren Versionsstand gehoben werden.

21 Daten- und Kommunikationskonzept

Vom Auftragnehmer (Anbieter, AN) sind bereits bei Angebotserstellung sowie bei einer allfälligen Leistungserbringung alle Kommunikationsbeziehungen mit Systemen und deren Datenspeicherung in den verfügbaren Formularen („Communication Matrix EN/GER“) unmissverständlich darzustellen und jedenfalls vor Beginn der Umsetzung vom Auftraggeber (AG) schriftlich freigeben zu lassen.

Dabei kann der AN zur besseren Verständlichkeit des Angebotes Einzelsysteme zu Gruppen gleichartiger Systeme zusammenfassen, wenn diese in Bezug auf Funktion, Kommunikationsbeziehungen sowie (Nicht-) Zugehörigkeit zum Liefer- und Leistungsumfang gleich sind. Spätestens in der (As-Built-) Dokumentation hat der AN für jedes System zu dokumentieren, zu welcher Gruppe gleichartiger Systeme es gehört.

Der AN haftet dem AG dafür, dass (unabhängig von einer allfälligen schriftlichen Freigabe) keine Kommunikationsbeziehung eingerichtet oder benutzt wird, die (a) zur rechtswidrigen Übermittlung geistigen Eigentums von voestalpine geeignet ist oder tatsächlich führt, oder (b), die Betriebs- oder IT-Sicherheit von Systemen oder Anlagen von voestalpine gefährden kann oder tatsächlich gefährdet. Allfällig vertraglich vereinbarte Haftungsausschlüsse und –Beschränkungen gelten in diesem Zusammenhang ausdrücklich nicht.

Für jeden einzelnen Verstoß gegen Punkt 21 hat der AN dem AG eine verschuldensunabhängige Konventionalstrafe in Höhe von 20% des Auftragswertes, mindestens jedoch EUR 20.000 zu leisten. Eine zu zahlende Konventionalstrafe wird auf einen allfälligen Schaden nicht angerechnet.

22 Verstöße

Verstöße gegen diese Anforderungen können zum sofortigen Entzug von Zugriffsrechten, zur Sperre von Mitarbeiterzugängen, zur Ablehnung der Leistung, zur Vertragskündigung aus wichtigem Grund sowie zu Schadenersatzforderungen führen.

23 ANHANG 1:
Mapping-Tabelle: Zusätzliche IT/OT-Sicherheitsanforderungen ↔ IEC 62443 / NIS2 (Auszug)

Kapitel / Anforderung	IEC 62443 relevante Teile	NIS2 – relevante Artikel / Anforderungen	Audit-Nachweis / Evidenz
Einhaltung von Industrienormen (NIS2 / IEC 62443)	IEC 62443-2-1 (IACS Security Program) IEC 62443-4-1 (Secure Product Development Lifecycle)	Art. 21 – Risikomanagement & Sicherheitsmaßnahmen Art. 23 – Rechenschaftspflicht	Sicherheitskonzept, Architektur-Dokumentation, Normen-Referenz
Security by Design / Security by Default	IEC 62443-4-1 (SR-1 bis SR-7) IEC 62443-3-2 (Risk Assessment)	Art. 21 Abs. 2 lit. a, c	Architektur-Reviews, Design-Freigaben
Verbot unautorisierter Netzwerkverbindungen	IEC 62443-3-3 (SR 1.1, SR 1.2, SR 2.1)	Art. 21 Abs. 2 lit. f (Zugriffskontrolle)	Netzwerkfreigaben, Firewall-Regeln
Netzwerk- & Systemzugriff nur nach Freigabe	IEC 62443-2-1 IEC 62443-3-3 (SR 1.x)	Art. 21 Abs. 2 lit. b, f	Freigabeprotokolle, Change-Management
Verbot von USB-Speichergeräten /Wechselmedien	IEC 62443-3-3 (SR 2.6 – Portable Media)	Art. 21 Abs. 2 lit. g (Asset Management)	Richtlinie Wechselmedien, technische Sperren
Kontrolle externer Datenträger	IEC 62443-2-1 (Policies & Procedures)	Art. 21 Abs. 2 lit. a	Policy-Dokumente, Schulungsnachweise
Verbot von Modems & drahtlosen Übertragungsgeräten	IEC 62443-3-3 (SR 5.1, SR 5.2 – Network Segmentation)	Art. 21 Abs. 2 lit. f	Netzwerktopologie, OT-Zonenmodell
Vermeidung unerlaubter Funk-/Fernzugriffe	IEC 62443-3-3 (SR 1, SR 5)	Art. 21 Abs. 2 lit. b, f	Technische Netzprüfungen
Pflicht zur IT/OT-spezifischen Sicherheits-Schulung	IEC 62443-2-1 (Awareness & Training)	Art. 21 Abs. 2 lit. i (Schulungen)	Schulungslisten, Zertifikate
Einsatzverbot ohne Schulungsnachweis	IEC 62443-2-1	Art. 21 Abs. 2 lit. i	Einsatzfreigaben, Personalnachweise
Nachweispflicht gegenüber dem AG	IEC 62443-2-1 (Compliance & Audit)	Art. 23 – Rechenschaftspflicht	Audit-Berichte, Lieferantenevaluierung
Remote-Access nur mit AG-Freigabe	IEC 62443-3-3 (SR 1, SR 2, SR 5)	Art. 21 Abs. 2 lit. f	Freigabelisten, Remote-Access-Policy
Gesicherter Fernzugriff	IEC 62443-3-3 (SR 1.13, SR 1.14)	Art. 21 Abs. 2 lit. c	Konfiguration, Protokolle

voestalpine
ONE STEP AHEAD.