Policy zum Einsatz von Zero Trust Architektur (ZTA) mit Künstlicher Intelligenz (KI) in Industrie 4.0

Version, Stand und Genehmigung

Dieses Dokument stellt die Version 3.0 der Policy zum Einsatz von Zero Trust Architektur mit Künstlicher Intelligenz dar, die am 22. Februar 2026 erstellt wurde. Es wurde von der Geschäftsführung, dem Chief Information Security Officer (CISO) und dem Datenschutzbeauftragten genehmigt, um eine maximale Auditierbarkeit zu gewährleisten. Die Genehmigung erfolgte durch Unterschriften, die in der gedruckten Version dieses Dokuments vorliegen, und dient als Nachweis für die formelle Annahme aller hierin festgelegten Regelungen.

Rahmenbedingungen und Geltungsbereich

Diese Policy gilt für alle Komponenten der Zero Trust Architektur sowie für alle Systeme der Künstlichen Intelligenz, die in der Organisation entwickelt, beschafft, betrieben oder eingesetzt werden. Sie umfasst insbesondere Anwendungen in operativen Technologien und Umgebungen der Industrie 4.0, wie etwa in der Produktion, der Lieferkette, der prädiktiven Wartung und der Qualitätskontrolle mit Unterstützung durch Künstliche Intelligenz. Die rechtliche und normative Grundlage dieser Policy basiert auf der EU AI Act in der Fassung der Verordnung (EU) 2024/1689, insbesondere den Artikeln 9 bis 15 für Systeme mit hohem Risiko gemäß Annex III, die Use-Cases in kritischer Infrastruktur, Beschäftigung und Produktqualitätssicherung betreffen. Darüber hinaus orientiert sie sich an der ISO/IEC 42001:2023 für das Artificial Intelligence Management System, an der ISO/IEC 27001:2022 für das Information Security Management System sowie an der IEC 62443 für die Sicherheit in operativen Technologien. Sie integriert die Prinzipien der NIST SP 800-207 für Zero Trust Architecture und der DoD Zero Trust Reference Architecture. Der Geltungsbereich ist auf Systeme mit Relevanz für Künstliche Intelligenz oder Zero Trust Architektur beschränkt, wobei Systeme mit niedrigem Risiko vereinfachte Regelungen unterliegen, die in separaten Anhängen dieses Dokuments detailliert beschrieben werden.

Ziele und Grundsätze

Die primären Ziele dieser Policy bestehen darin, den sicheren, verantwortungsvollen und konformen Einsatz von Zero Trust Architektur und Künstlicher Intelligenz in industriellen Umgebungen zu gewährleisten. Es soll die Integrität, Verfügbarkeit und Vertraulichkeit von Daten und Systemen geschützt werden, während gleichzeitig die Nachvollziehbarkeit und Resilienz gegenüber Cyberbedrohungen erhöht wird. Alle regulatorischen Anforderungen der EU AI Act und der ISO 42001 werden vollständig eingehalten. Die Grundsätze dieser Policy orientieren sich an den Kernprinzipien der NIST Zero Trust Architecture und der ISO 42001 Annex A. Es gilt das Prinzip, niemals blind zu vertrauen, sondern immer explizit zu verifizieren, was durch dynamische und kontextbasierte Authentifizierung umgesetzt wird. Ein Angriff wird stets vorausgesetzt, was eine kontinuierliche Überwachung und die Vergabe minimaler Privilegien erfordert. Die Provenienz von Daten und Entscheidungen muss über den gesamten Lebenszyklus hinweg gesichert sein. Eine menschliche Aufsicht ist bei Entscheidungen mit hohem Risiko obligatorisch. Der kontinuierliche Verbesserungsprozess folgt dem Plan-Do-Check-Act-Zyklus, der in allen Prozessen dieser Policy verankert ist.

Motivation für den Einsatz von ZTA und KI

Der Einsatz von Zero Trust Architektur kombiniert mit Künstlicher Intelligenz in der Industrie 4.0 dient der Erhöhung der Sicherheit in vernetzten Produktionsumgebungen, in denen traditionelle Perimeter-Sicherheit nicht mehr ausreicht. Durch dynamische Verifizierung und KI-gestützte Kontextanalyse können Bedrohungen frühzeitig erkannt und minimiert werden. Diese Policy stellt sicher, dass der Einsatz ethisch, rechtlich und technisch verantwortungsvoll erfolgt und Risiken für Betriebssicherheit, Datenschutz und Grundrechte minimiert werden.

Zugriffssteuerung

Die Zugriffssteuerung erfolgt ausschließlich dynamisch und kontextbasiert gemäß den Prinzipien der Zero Trust Architektur. Jeder Zugriffsversuch wird vollständig verifiziert, unabhängig von Netzwerkposition oder vorheriger Authentifizierung. In der folgenden Tabelle werden die wesentlichen Anforderungen an die Zugriffssteuerung detailliert beschrieben, wobei jede Zelle vollständige Sätze enthält.

Anforderung an die Zugriffssteuerung	Beschreibung der Anforderung	Umsetzungsverpflichtung	Verantwortlicher Bereich
Dynamische Policy-Durchsetzung	Jeder Zugriff wird in Echtzeit anhand aktueller Kontextdaten (Identität, Gerät, Ort, Zeit, Verhalten) bewertet und genehmigt oder abgelehnt.	Diese Anforderung ist verpflichtend für alle Systeme mit hohem Risiko.	Chief Information Security Officer und DevOps-Team
Least Privilege Prinzip	Jeder Benutzer, jedes Gerät und jede Anwendung erhält nur die minimal notwendigen Rechte, die für die jeweilige Aufgabe erforderlich sind.	Diese Anforderung ist verpflichtend und wird durch automatisierte Policy-Engines umgesetzt.	Fachabteilungen und Security-Team
Policy Decision Point und Enforcement	Ein zentraler Policy Decision Point trifft die Entscheidung, während Policy Enforcement Points die Durchsetzung vor Ort übernehmen.	Diese Architekturkomponenten müssen in allen relevanten Systemen implementiert sein.	IT-Architektur und OT-Security
Multi-Factor-Authentifizierung	Für alle Zugriffe auf sensible Ressourcen ist eine starke Multi-Factor-Authentifizierung obligatorisch.	Diese Anforderung gilt ohne Ausnahme für High-Risk-Systeme.	Identity- und Access-Management-Team

Integrität und Datenprovenienz

Die Integrität von Daten und Entscheidungen wird durch kontinuierliche Überwachung und kryptografische Maßnahmen sichergestellt. Die Provenienz aller Daten, die in KI-Systemen oder ZTA-Komponenten verwendet werden, muss nachvollziehbar und unveränderbar dokumentiert sein. In der folgenden Tabelle werden die Anforderungen an Integrität und Provenienz detailliert beschrieben.

Anforderung an Integrität und Provenienz	Beschreibung der Anforderung	Umsetzungsverpflichtung	Verantwortlicher Bereich
Datenprovenienz über Lifecycle	Die Herkunft, Veränderung und Nutzung aller Daten muss lückenlos protokolliert werden.	Diese Anforderung ist verpflichtend gemäß EU AI Act Art. 10 und ISO 42001 A.7.	Datenschutzbeauftragter und Data-Governance-Team
Integritätsprüfung in Echtzeit	Alle Datenströme und KI-Entscheidungen werden auf Integrität geprüft, inklusive Hashing und Signaturen.	Diese Anforderung gilt für alle OT- und IT-Datenflüsse.	Security-Operations-Center
Bias-Mitigation und Qualitätskontrolle	Datenqualität und Bias werden kontinuierlich überwacht und gemindert.	Diese Anforderung ist verpflichtend für High-Risk-KI-Systeme.	AI Ethics Officer

Nachvollziehbarkeit und Transparenz

Alle Entscheidungen der Künstlichen Intelligenz sowie alle Zugriffsentscheidungen der Zero Trust Architektur müssen nachvollziehbar und erklärbar sein. In der folgenden Tabelle werden die Anforderungen an Nachvollziehbarkeit detailliert beschrieben.

Anforderung an Nachvollziehbarkeit	Beschreibung der Anforderung	Umsetzungsverpflichtung	Verantwortlicher Bereich
Audit-Logs und Explainability	Jede Entscheidung wird protokolliert und erklärbar gemacht, inklusive Model Cards für KI-Modelle.	Diese Anforderung ist verpflichtend gemäß EU AI Act Art. 13 und ISO 42001 A.8.	AI Development und Audit-Team
Kontinuierliche Dokumentation	Alle relevanten Ereignisse und Kontextdaten werden zeitlich gestempelt und unveränderbar gespeichert.	Diese Anforderung gilt für mindestens 5 Jahre.	Compliance und Legal

Sicherheit und kontinuierliche Überwachung

Die Sicherheit wird durch kontinuierliche Überwachung, Incident-Response und automatisierte Maßnahmen gewährleistet. In der folgenden Tabelle werden die Anforderungen an Sicherheit detailliert beschrieben.

Anforderung an Sicherheit	Beschreibung der Anforderung	Umsetzungsverpflichtung	Verantwortlicher Bereich
Kontinuierliche Überwachung	Alle Aktivitäten werden in Echtzeit überwacht, Anomalien werden automatisch erkannt.	Diese Anforderung ist verpflichtend gemäß NIST SP 800-207 und IEC 62443.	Security-Operations-Center
Incident Management	Bei Sicherheitsvorfällen wird ein definierter Response-Prozess aktiviert, inklusive CAPA.	Diese Anforderung gilt für alle Incidents.	CISO und Incident-Response-Team
Micro-Segmentation	Netzwerke und Ressourcen sind mikro-segmentiert, um Lateral Movement zu verhindern.	Diese Anforderung ist verpflichtend in OT-Umgebungen.	Netzwerk- und OT-Team

Review, Aktualisierung und Verantwortlichkeiten

Diese Policy wird mindestens jährlich sowie bei signifikanten Änderungen, neuen regulatorischen Anforderungen oder Incidents überprüft und aktualisiert. Der Review-Prozess umfasst eine Bewertung der Wirksamkeit und eine Anpassung an neue Risiken. In der folgenden Tabelle werden die Key Performance Indicators detailliert beschrieben.

Key Performance Indicator	Beschreibung des Indicators	Zielwert, der für diesen Indicator festgelegt ist

Prozentsatz dynamisch verifizierter Zugriffe	Dieser Indicator misst den Anteil der Zugriffe, die vollständig dynamisch verifiziert wurden.	Der Zielwert für diesen Indicator beträgt 100 Prozent.
Time-to-Detect für Anomalien	Dieser Indicator misst die Zeit bis zur Erkennung von Anomalien oder Verletzungen.	Der Zielwert für diesen Indicator liegt unter 5 Minuten.
Prozentsatz nachvollziehbarer KI-Entscheidungen	Dieser Indicator misst den Anteil erklärbarer und protokollierter Entscheidungen.	Der Zielwert für diesen Indicator beträgt über 95 Prozent.

Der kontinuierliche Verbesserungsprozess umfasst Lessons Learned, Management Reviews und Corrective Actions gemäß ISO 42001 Clause 9 und 10, die in Protokollen dokumentiert werden.

Anhang: Referenzen und Changelog

Die Referenzen umfassen die EU AI Act unter https://artificialintelligenceact.eu, die NIST SP 800-207, die ISO/IEC 42001:2023 mit Annex A, die DoD Zero Trust Reference Architecture sowie die IEC 62443-Serie. Der Changelog dokumentiert Änderungen: In Version 3.0 wurden alle Inhalte zu vollständigen Sätzen und Tabellen erweitert, um maximale Auditierbarkeit und juristische Lesbarkeit zu gewährleisten, einschließlich Mapping zu Standards und formaler Strukturen.