



GLOBALE POLICY ZUR INFORMATIONSSICHERHEIT

Dieses Dokument legt den Unternehmensansatz in Bezug auf Informationssicherheit fest, im Einklang mit der strategischen Ausrichtung des Unternehmens und den geltenden gesetzlichen, regulatorischen¹ und vertraglichen Anforderungen an die Sicherheit von Netzwerk- und Informationssystemen.

Diese Policy wird regelmäßig überprüft und gegebenenfalls aktualisiert, um den geltenden regulatorischen Anforderungen gerecht zu werden und sich an die wandelnde Risikolandschaft anzupassen, sofern neue Arten von Bedrohungen für Unternehmensinformationen entstehen.

PRINZIPIEN

In dieser Policy werden insbesondere die wichtigsten Prinzipien zum Schutz der Informationswerte der Organisation definiert:

- **„Vertraulichkeit“**, d. h. die Fähigkeit sicherzustellen, dass der Zugriff auf Informationen oder deren Offenlegung ausschließlich auf hierzu berechnigte Personen oder Einrichtungen beschränkt ist;
- **„Integrität“**, d. h. die Fähigkeit, die Richtigkeit und Vollständigkeit der Informationen im Laufe der Zeit zu gewährleisten;
- **„Verfügbarkeit“**, d.h. die Fähigkeit, Informationen innerhalb der erforderlichen Zeiträume und in der von berechtigten Personen oder Einrichtungen benötigten Art und Weise verfügbar, zugänglich und nutzbar zu machen.

Diese Prinzipien bilden einen Rahmen für das Management von Risiken, die Unternehmensinformationen und -werte (Anwendungen, Dienste, Infrastruktur oder andere Komponenten, die Informationen verarbeiten) beeinträchtigen können, und schützen diese vor internen oder externen, vorsätzlichen oder unbeabsichtigten Bedrohungen.

Diese Policy verpflichtet die Mitarbeiter des Konzerns, Lieferanten (einschließlich ihrer Subunternehmer), Mitarbeiter von Fremdfirmen sowie allen Dritten, die mit Daten, Informationen oder Informationssystemen von Pirelli umgehen, die Einhaltung in dieser Policy festgelegten Prinzipien sowie aller geltenden Gesetze und Vorschriften

Die Sicherheit des Pirelli-Konzerns basiert auf wesentlichen Grundsätzen wie kontinuierlicher Risikobewertung, dem Schutz kritischer Informations- und IT-Werte, der Schulung von Personal und der Fähigkeit zur Reaktion auf Vorfälle.

Um ein wirksames Informationssicherheitsmanagement im Einklang mit den in dieser Richtlinie festgelegten Grundsätzen zu gewährleisten, wendet der Pirelli-Konzern ein robustes und strukturiertes Rahmenwerk an, das durch spezifische interne Verfahren und Betriebsanweisungen die Rollen, Verantwortlichkeiten und operativen Abläufe im Zusammenhang mit der Informationssicherheit festlegt.

¹ Aus diesem Grund definieren, implementieren und überwachen die Unternehmen der Pirelli-Gruppe, die der Richtlinie (EU) 2022/2555 (NIS2) unterliegen, die geltenden Anforderungen im Rahmen ihres Organisations- und Verfahrensrahmens, der aus Policies, Standards, Operating Procedure und Guidelines besteht.

GOVERNANCE, RISIKOMANAGEMENT UND KONTINUIERLICHE VERBESSERUNG

Das Board of Directors der Pirelli & C. S.p.A. ist für die Genehmigung dieser Policy für Informationssicherheit und Cybersecurity, im Einklang mit den geltenden regulatorischen Anforderungen, einschließlich der NIS2-Richtlinie, verantwortlich.

Das Top Management des Konzerns ist mit Unterstützung des Funktionsbereichs Information Security sowie weiterer relevanter Unternehmensfunktionen für die vollständige Umsetzung dieser Policy verantwortlich und stellt die wirksame Einführung von Sicherheitsmaßnahmen sowie geeignete Berichtswege an das Board of Directors sicher.

Das interne Kontrollsystem des Pirelli-Konzerns ist darauf ausgerichtet, eine korrekte Berichterstattung und angemessene Kontrollen über sämtliche Aktivitäten des Konzerns sicherzustellen wobei Bereichen, die als potenziell risikobehaftet gelten, besondere Aufmerksamkeit gewidmet wird. Dies erfolgt durch einen Risikomanagementprozess, der auch Cybersecurity-Risiken des Konzerns und relevanter Dritter umfasst. Der Pirelli-Konzern identifiziert die erforderlichen Maßnahmen um seine Sicherheitslage, sein Risikomanagement und die Einhaltung der regulatorischen Anforderungen kontinuierlich zu verbessern sowie die Umsetzung ihrer internen Richtlinien zur Informationssicherheit sicherzustellen.

ÜBERWACHUNG VON SICHERHEITSEREIGNISSEN, REAKTION AUF SICHERHEITSVORFÄLLE UND KRISENMANAGEMENT

Der Pirelli-Konzern verfolgt einen strukturierten und integrierten Sicherheitsansatz auf Grundlage formalisierter Prozesse zur kontinuierlichen Überwachung von Sicherheitsereignissen, zum Schwachstellenmanagement sowie zur Reaktion auf Sicherheitsvorfälle und Krisenereignisse.

Insbesondere identifiziert, analysiert, priorisiert und der Pirelli-Konzern Schwachstellen, die Informationssystemen betreffen, und legt geeignete Maßnahmen zu deren Behandlung fest. Sie überwacht und analysiert Sicherheitsereignisse um Bedrohungen, die die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen beeinträchtigen könnten, frühzeitig zu erkennen und angemessen zu adressieren. Darüber hinaus werden Incident-Response-Pläne eingesetzt, die den gesamten Prozess von der Erkennung eines Sicherheitsvorfalls bis hin zu den erforderlichen Korrekturmaßnahmen zur Verringerung der Wiederholungswahrscheinlichkeit abdecken. Die beteiligten Rollen, Kommunikationskanäle und Eskalationsverfahren sind Bestandteil eines strukturierten und formalisierten Prozesses, der sowohl externe als auch interne Kommunikationswege umfasst.

Der Pirelli-Konzern verfügt über Krisenmanagementprozesse (einschließlich für schwerwiegende Vorfälle) mit Eskalation zu Business-Continuity-Plänen, die die Festlegung und Umsetzung schneller und wirksamer Maßnahmen als Reaktion auf unvorhergesehene und/oder außergewöhnliche Ereignisse ermöglichen, mit dem Ziel, den Betrieb so schnell wie möglich wiederherzustellen und potenzielle Schäden zu minimieren.

INTEGRIERTES KONTROLLSYSTEM FÜR INFORMATIONSSICHERHEIT

Der Pirelli-Konzern definiert und unterhält ein abgestimmtes Bündel technischer, organisatorischer und personeller Maßnahmen als Ergänzung seines Informationssicherheits-Managementsystems. In diesem Zusammenhang definiert und pflegt die Gruppe unter anderem Schulungs- und Sensibilisierungsprogramme für Mitarbeiter und Dritte (sofern zutreffend), führt Prozesse zur Klassifizierung und zum Schutz von Informationen ein und gewährleistet das sichere Management von Informations- und IT-Werten einschließlich ihres physischen Schutzes über deren gesamten Lebenszyklus hinweg.

Gleichzeitig wendet der Konzern strukturierte Modelle zur Verwaltung digitaler Identitäten und Zugriffskontrollen an, die sicherstellen sollen, dass Nutzer zur Nutzung von IT-Ressourcen berechtigt sind und nur auf die Informationen zugreifen, die zur Erfüllung ihrer Aufgaben erforderlich sind („Need-to-know“), wobei Berechtigungen nur im unbedingt notwendigen Umfang vergeben werden („Least

Privilege“). Zudem schützt der Konzern seine physische Infrastruktur und integrierte Sicherheitsprinzipien gemäß einem „Security-by-Design“ Ansatz in dem Lebenszyklus von Informationssystemen. Unternehmensnetzwerke und -kommunikation werden zusätzlich durch technische Schutz- und Segmentierungslösungen geschützt, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.

MELDUNGEN, VERTRAULICHKEIT, KEINE REPRESSALIEN UND KONSEQUENZEN BEI VERSTÖßEN

Der Pirelli-Konzern ermutigt die Empfänger dieses Dokuments, in gutem Glauben, auch anonym, jede Handlung oder Unterlassung einer Person bei Pirelli, in Beziehungen zu Pirelli oder in ihrem Namen zu melden, die einen Verstoß gegen die in dieser Policy enthaltenen Grundsätze darstellt oder darstellen könnte oder zu einem solchen Verstoß verleitet. Die „[Whistleblowing Policy](#)“, die auf der Website www.pirelli.com in mehreren Sprachen veröffentlicht ist, legt das Verfahren für die Einreichung von Hinweisen fest, wie diese gehandhabt werden und wie Vertraulichkeit und der Schutz vor Repressalien gewährleistet werden.

Pirelli ergreift im Falle eines Verstoßes gegen diese Policy angemessene Maßnahmen, unabhängig davon, ob diese durch das Whistleblowing-Verfahren oder auf anderem Wege aufgedeckt wurden. Je nach Schweregrad können dies Korrekturmaßnahmen (unter anderem: Gespräch mit dem betroffenen Mitarbeiter, Erstellung eines konkreten Aktionsplans mit den zuständigen Führungskräften usw.) und/oder disziplinarische Maßnahmen (unter anderem: mündliche und/oder schriftliche Verweise, negative Leistungsbeurteilungen oder Kündigung) umfassen, jeweils im Einklang mit den geltenden vertraglichen, disziplinarischen, gesetzlichen und regulatorischen Vorschriften.

DOKUMENTE IM ZUSAMMENHANG MIT DIESER POLICY

- [CODE OF ETHICS](#) und [CODE OF CONDUCT](#)
- [GLOBAL PERSONAL DATA PROTECTION POLICY](#)
- [INTELLECTUAL PROPERTY POLICY](#)
- [WHISTLEBLOWING POLICY](#)

September 2026

PIRELLI & C. S.p.A.
BOARD OF DIRECTORS