

Grundsatzenerklärungen

Vulcan Energy verpflichtet sich zum Schutz seiner digitalen Vermögenswerte, der Betriebstechnologie, der Informationssysteme, der Daten sowie der Mitarbeiterinformationen. Diese Richtlinie legt die Grundsätze, Verantwortlichkeiten und Mindestanforderungen fest, mit denen das Unternehmen vor Cyberbedrohungen geschützt wird und eine starke Governance, operative Resilienz sowie die Einhaltung regulatorischer Anforderungen unterstützt werden.

Vulcan Energy verfolgt dieses Ziel insbesondere durch:

- Einhaltung aller anwendbaren Gesetze und Vorschriften zu Cybersicherheit, Datenschutz, Privatsphäre und kritischer Infrastruktur sowie durch interne Prozesse zur Überwachung und Umsetzung regulatorischer Änderungen.
- Durchführung von Cybersicherheits-Risikobewertungen im Einklang mit ISO 27001, ISO 31000 und dem Vulcan Risk Management Standard.
- Pflege eines aktuellen Cyber-Risikoregisters, das sowohl Risiken der Informationstechnologie (IT) als auch der Betriebstechnologie (OT) abdeckt.
- Schutz von OT- und industriellen Steuerungssystemen durch geeignete Segmentierung, Zugriffskontrollen und Überwachung.
- Anwendung von „Security-by-Design“-Prinzipien bei neuen Systemen, Tools und Infrastrukturen.
- Bereitstellung eines erhöhten Schutzniveaus für kritische Systeme, insbesondere in Bezug auf Sicherheit, Umweltintegrität, Produktion und regulatorische Verpflichtungen.
- Durchführung regelmäßiger Cybersicherheitsaudits, Schwachstellenanalysen und unabhängiger Penetrationstests zur Überprüfung der Wirksamkeit der Kontrollen.
- Sicherstellung rollenbasierter Zugriffskontrollen sowie regelmäßiger Überprüfung der Zugriffsrechte.
- Verschlüsselung sensibler Informationen zum Schutz vor unbefugtem Zugriff.
- Angemessene Klassifizierung und Handhabung von Informationen entsprechend ihrer Sensibilität.
- Implementierung von Multi-Faktor-Authentifizierung (MFA), sofern technisch umsetzbar.
- Überwachung und Erkennung von Cyberbedrohungen sowie Sicherstellung des Einsatzes geeigneter Tools und Prozesse zur Identifikation und Reaktion auf Bedrohungen.
- Absicherung interner und externer Netzwerke durch Firewalls sowie Systeme zur Erkennung und Verhinderung von Eindringversuchen.
- Zeitnahe Bereitstellung von Sicherheitsupdates und Patches sowie Nachverfolgung und Behebung kritischer Schwachstellen innerhalb definierter Fristen.
- Sicherstellung sicherer Konfigurations- und Änderungsmanagement-Praktiken für Systeme und Infrastrukturen.
- Bereitstellung verpflichtender Schulungen zu Cybersicherheit und Datenschutz, angepasst an die jeweiligen Rollen, einschließlich regelmäßiger Auffrischungen.
- Aufrechterhaltung von Incident-Response- und Business-Continuity-Plänen zur Gewährleistung der Einsatzbereitschaft bei Cyberfällen und Datenschutzverletzungen.
- Durchführung einer risikobasierten Lieferanten-Due-Diligence sowie Aufrechterhaltung geeigneter Überwachungs- und Kontrollmechanismen für Lieferanten, Dienstleister und sonstige Dritte, die Zugriff auf die Systeme oder Daten von Vulcan haben.

Cybersicherheit ist ein zentraler Bestandteil des unternehmensweiten Risikomanagementansatzes von Vulcan. Sie spiegelt den konservativen, risikobasierten Ansatz des Unternehmens im Umgang mit Cyber- und OT-Risiken wider und ist vollständig in das Vulcan Risk Management Framework integriert.

Verantwortung und Rechenschaftspflicht

Diese Richtlinie wird jährlich überprüft und gilt für alle Vorstandsmitglieder, Mitarbeitenden, Auftragnehmer, Berater sowie sonstige Drittpersonen, die bei Vulcan tätig sind. Der Vulcan-Vorstand trägt die letztendliche Verantwortung für die Cyber-Resilienz. Das Audit, Risk & ESG Committee übernimmt die Aufsicht über Cyberrisiken, die Wirksamkeit der Kontrollen, Vorfälle sowie Assurance-Aktivitäten.

Der Chief Information Officer ist für die operative Cybersicherheit, das Monitoring sowie die Umsetzung der Kontrollen verantwortlich. Mitarbeitende und Auftragnehmer tragen gemeinsam Verantwortung für sicheres Verhalten und die Einhaltung dieser Richtlinie.

Der Chief Executive Officer der Vulcan Group ist gegenüber dem Vorstand dafür verantwortlich, dass diese Richtlinie umgesetzt und eingehalten wird.



Cris Moreno

Geschäftsführer und CEO

Referenz	Genehmigende Stelle	Genehmigungsdatum
PL-0772 V0	Vulcan Board	30 März 2026