Cybersecurity Policy

Policy Commitments

Vulcan Energy is committed to protecting its digital assets, operational technology, information systems, data, and employee information. This Policy sets out the principles, responsibilities and minimum requirements that safeguard the Company from cyber threats and support strong governance, operational resilience, and regulatory compliance.

Vulcan Energy aims to achieve this by:

- Complying with all applicable cybersecurity, privacy, data protection and critical-infrastructure laws and regulations, and maintaining internal processes to monitor and implement regulatory changes.
- Implementing cybersecurity risk assessments aligned with ISO 27001, ISO 31000 and the Vulcan Risk Management Standard.
- Maintaining an up-to-date cyber risk register covering both Information Technology (IT) and Operational Technology (OT) risks.
- Protecting OT and industrial control systems through appropriate segmentation, access controls and monitoring.
- Applying security-by-design principles in new systems, tools and infrastructure.
- Providing enhanced protection for critical systems, including those relating to safety, environmental integrity, production and regulatory obligations.
- Conducting regular cybersecurity audits, vulnerability assessments and independent penetration tests to ensure control effectiveness.
- Ensuring role-based access controls and conducting periodic access reviews.
- Encrypting sensitive information to prevent unauthorised access.
- Applying appropriate classification and handling of information based on sensitivity.
- Implementing multi-factor authentication (MFA) where technically feasible.
- Monitoring and detecting cybersecurity threats, ensuring the use of appropriate tools and processes for threat identification and response.
- Securing internal and external networks using firewalls and intrusion detection/prevention systems.
- Ensuring timely deployment of security updates and patches, and tracking and remediation of critical vulnerabilities within defined timeframes.
- Ensuring secure configuration and change management practices for systems and infrastructure.
- Providing mandatory cybersecurity and privacy training appropriate to employee roles, with periodic refreshers.
- Maintaining incident response and business continuity plans, ensuring readiness for cyber events and data breaches.
- Performing due diligence and ongoing monitoring of suppliers, vendors and third parties with access to Vulcan systems or data.

Cybersecurity is a core element of Vulcan's enterprise risk management approach, reflecting the Company's conservative risk-based approach to cyber and OT risks, and is fully integrated into Vulcan's Risk Management Framework.

Responsibility and accountability

This policy will be reviewed annually and applies to all Vulcan Group directors, employees, contractors, consultants and any third-party workers employed at Vulcan operations. The Vulcan Board retains ultimate accountability for cyber resilience with the Audit, Risk & ESG Committee providing oversight of cybersecurity risk, control effectiveness, incidents, and assurance activities. The Chief Information Officer is responsible for operational cybersecurity, monitoring, and control execution with employees and contractors sharing responsibility for secure behaviours and compliance with this Policy.

The Chief Executive Officer of Vulcan Group is accountable to the Board for ensuring this policy is implemented and adhered to.

Cris Moreno
Managing Director and CEO

Reference	Approving Authority	Approved Date
PL-0773 V0	Vulcan Board	30 March 2026