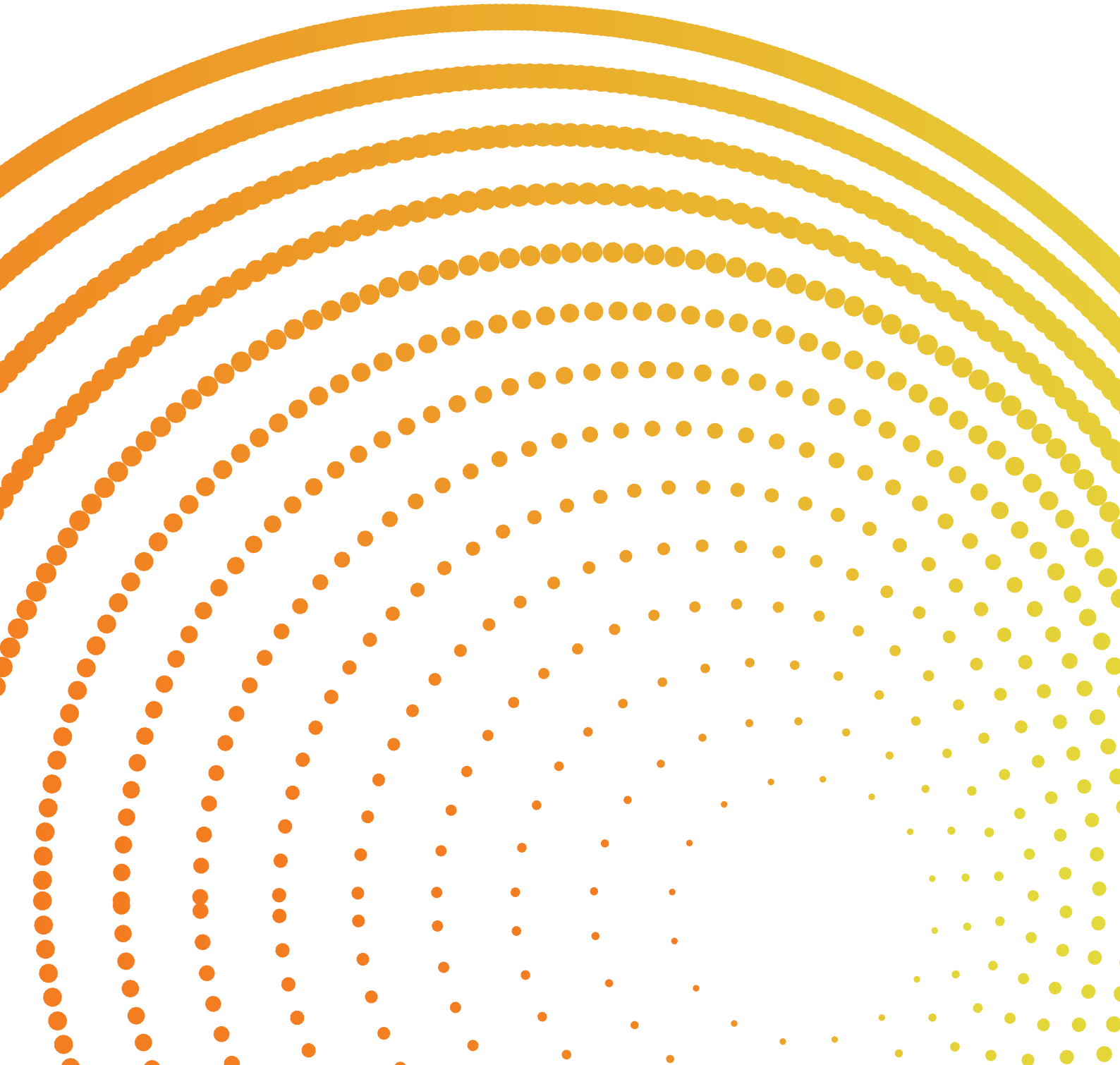
Cyber Security Statement 2022

Molycop Legal



Molycop's Cyber Security Statement

Molycop is dedicated to protecting the assets and information that is owned or entrusted to us by customers, business partners, and employees; therefore, we place great importance on information security, including cyber security, to protect against external threats and malicious insiders. Molycop's cyber security strategy prioritizes detection, analysis, and response to known, anticipated, or unexpected cyber threats, effective management of cyber risks, and resilience against cyber incidents. Molycop continuously strives to meet or exceed the industry's information security best practices and applies controls to protect our clients and Molycop. Molycop maintains a formal cyber security program structured around the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and the related industrial services sector cyber security profile.

This document provides an overview of Molycop's approach to information security and its practices to secure data, systems, and services, similarly aligned around the five functions of the NIST CSF:

Identify

- **Risk Governance and Oversight**

  Risk management is a function of Molycop's management culture, embedded practices and formal oversight. Molycop's governance model is achieved by the day-to-day activities of managers and their teams, supported by various working groups.

- **Information Security and Cyber Security Policies and Procedures**

  Molycop maintains a comprehensive set of information security policies and procedures to document the company's approach to compliance with laws, rules, regulations, best practices, and Molycop management directives.

- **Asset Management**

  Molycop maintains an asset management program to appropriately inventory, classify, and protect applications, data, and hardware.

Protect

- **Training and Awareness**

  Molycop provides all employees with annual cyber security awareness training. Additional targeted training is delivered periodically and in a timely manner to ensure personnel maintain awareness of evolving cyber threats and countermeasures.

- **Identity and Access Management**

  Molycop has implemented controls to identify, authorize, authenticate, and manage individuals' access to our systems and information assets.

- **Application and Software Security**

  Molycop manages application and software security through its software management process which includes a centralized inventory, vulnerability testing, control monitoring, and logging.

- **Infrastructure Security**

  Molycop protects its infrastructure through a control framework which includes architecture reviews, vulnerability testing, system hardening, and malware protection.

- **End User Device Security**

  Molycop's mobile solutions allow employees to conduct business activities on their personal devices while protecting Molycop systems and client data.

- **Data Protection and Data Privacy**

  Molycop has implemented controls designed to safeguard our company and client information which covers data classification, secure storage, handling, transmission, and destruction.

- **Physical Security**

  Molycop has implemented physical access controls at all Molycop facilities including office spaces, near site and far site locations, data centers, and storage facilities.

- **Vendor Security**

  Information security risk management is built into Molycop's vendor management process, which covers vendor selection, onboarding, performance monitoring, and risk management.

Detect

- **Continuous Monitoring**

  Molycop maintains detective controls at the network, endpoint, and application layers to detect anomalous activity potentially indicative of threat activity. We further implement continuous control monitoring to assess the adoption and performance of security controls.

- **Anomaly Detection**

  Molycop ensures that security anomalies and events are detected quickly, and their potential impact is understood.

- **Enforcing Protective Measures**

  Molycop tests and confirms all protective security measures to verify the effectiveness and coverage.

Respond

- **Security Incident Management**

  Molycop's security incident management program enables effective detection and management of security threats and incidents that have a potential impact on the confidentiality, integrity, or availability of Molycop's information and technology environment, including notification to customers or employees as required by applicable laws and regulations.

- **Response Planning**

  Molycop incorporates coordinated response planning processes during and after any security incidents, which include managing communications and analyzing the effectiveness of response activities.

Recover

- **Business Continuity and Industrial Resilience**

  Molycop has global Disaster Recovery and Business Continuity Programs (DR/BCP). The program covers both business and industrial resilience. The main features of the program include dispersed capabilities, near site recovery, far site recovery, and dispersed recovery.

While information security measures will naturally change over time and may differ across the range of Molycop's services and sites, this document provides an overview of our security practices.

Information Security Program

- Molycop maintains an Information Security Program, which consists of a centralized global team to establish information security mandates, evaluate compliance, and detect and respond to incidents, along with the local teams embedded in each operating division. The program is frequently adjusted to ensure ongoing suitability.
- The Information Security Program regularly assesses the sufficiency of Molycop's controls. In particular, the Program administers an annual cyber security maturity assessment using external resources.
- Molycop's Director of Global Information Security is responsible for managing and implementing the Information Security Program and reports directly to the Chief Information Officer. The Director of Global Information Security is responsible for setting company-wide control requirements, assessing adherence to controls, identifying, and prioritizing cyber security risks, and detecting and responding to incidents. The CIO in coordination with the Director of Global Information Security report quarterly to the Board of Directors concerning the overall status of the information security program.
- The written Information Security Program is approved by Molycop's Leadership, annually. The Leadership Team takes an active interest in information security and cyber security matters and sets the Molycop's risk appetite in these areas, monitors progress, and receives regular updates

Policies and Procedures

- Molycop maintains a comprehensive set of information security and cybersecurity policies and procedures which take into consideration data privacy laws and regulations including data retention requirements.
- Policies and procedures are reviewed and approved by senior management. The Global Information Security and Cybersecurity Program and Policy are reviewed annually. Other policies and standards are reviewed at least every three years.
- Molycop policies and procedures are aligned with National Institute of Standards and Technology (NIST).
- Molycop policies and procedures are available to all Molycop Employees. These policies cover all aspects of the Information Security Program. Topics governed by information and cybersecurity policies and procedures include, but are not limited to:

  – Access Control Policy defining standards and requirements for connecting to Molycop systems and information.

  – Acceptable Use Policy which is focused on employee care and use of company resources, applications, and data.

  – Network Security Policy which defines minimum and recommended standards for each part of the network including endpoint security, wired and wireless communications.

  – Mobile Device Management Policy which outlines requirements and expectations of any mobile device regardless of corporate or personal ownership.

  – Vulnerability and Patch Management Policy outlines the required and expected practices regarding application of security updates and vulnerability remediation to minimize risk.

MOLYCOP

molycop.com