Cyber Security Policy

Dyno Nobel Limited is committed to protecting the confidentiality, integrity and availability of our information and technology assets. Information security is essential to maintaining the trust of our employees, customers, partners and shareholders .We recognise that cyber threats, emerging technologies (including artificial intelligence), and increasing digital interconnectivity require a proactive, risk based and continuously improving approach to information security.

Dyno Nobel is committed to actively enhancing its cyber capabilities over time, acknowledging that maturity is an ongoing journey rather than a fixed state.

The Audit and Risk Management Committee (ARMC) of the Board has oversight of information security. At the management level, operational accountability is shared between the Chief Information Officer and General Manager Cyber & Governance Global.

We are committed to

- Continually working to improve our information security governance, policies, systems and controls to address evolving threats, business needs and technology changes.
- Monitoring, detecting and responding to information security threats and incidents to minimise harm to the business, our people and stakeholders.
- Regular internal reporting on information security performance, risks and incidents to support governance, accountability and informed decision making across business leadership, including the Audit and Risk Management Committee of the Board.

Core Principles

Artificial Intelligence:

We are committed to:

· Progressively strengthening the responsible, secure and ethical use of AI and automated decision making technologies as our capabilities and understanding evolve.

· Continuously improving the way we assess and manage information security and data risks associated with the use, development, and deployment of AI solutions, adapting our approach as threats, regulations and business needs evolve.

People & Responsibilities

We are committed to:

· Maintaining established responsibilities for information security via policies, standards and procedures.

· Providing appropriate training and awareness to ensure responsibilities are understood and employees are equipped to act securely.

· Fostering a strong security culture where employees feel empowered to speak up, report concerns and challenge unsafe or non-compliant practices.

Third Parties:

We are committed to:

· Continually improving our assessment and management of third party information security risks as part of procurement, onboarding and ongoing relationship management.

· Seeking to require relevant third parties to agree to security, privacy and contractual obligations.

Application

This Cyber Security Policy applies to all Dyno Nobel operations, including wholly owned subsidiaries of Dyno Nobel.