Security Risk Policy Statement

As an innovative industry leader, Vestas strives to secure sustainable energy ecosystems, protecting the value of the global energy transformation. Recognizing the increasing complexity of digitalization and threats, Vestas highlights risk management as an important driver that caters for appropriate protection, especially for our personnel, data, locations, deliveries, and stakeholders.

Policy purpose

With this policy and the four principles below, Vestas expects to deliver reliable, scalable, and resilient energy solutions:

- Aware: Vestas trains the workforce, advancing accountability for security.
- Credible: Vestas acts with integrity, delivering with the respect we have for our surroundings.
- Available: Vestas operates with quality, supporting consistent delivery of value.
- Flexible: Vestas embraces modularity, offering solutions based on our harmonized product base.

Scope

Vestas is committed to protecting the value we create through global energy transformation. To sustain our industry leadership, we must embrace robust standards that protect our staff, company, customers, and shareholders. Recognizing our industrial role, we also acknowledge the high expectations of our global partners in sustainable energy.

This policy applies to all of Vestas.

Roles & Responsibilities

The following defines the overarching mandates required to maintain clear accountability: The Board of Directors is responsible for setting the risk profiles for security in Vestas. The Executive Management is responsible for approving risk management strategies.

Vestas Wind Systems A/S
Hedeager 42 . 8200 Aarhus N . Danmark
Tlf: +45 9730 0000 . Fax: +45 9730 0001
vestas@vestas.com . vestas.com

The Audit functions are responsible for delivering a risk-based and independent assurance of the organization's security and risk management practices

This includes:
- Establish audit plans as appropriate for the organization's risk profile.
- Conducting independent assessments of security programs and risk management controls.
- Reporting the audit results to Board of Directors and senior management.

The Chief Information Security Officer (CISO) is responsible for upholding a risk-based security at Vestas.

This includes:
- A risk-based and customer centric approach that enables security capabilities and outcomes.
- An effective and efficient security organisation and management system.
- Reporting the organization's risk landscape, threats, and cybersecurity posture to the Board of Directors and governing entities.

All managers are responsible for exercising risk control within their respective domains. They are responsible for managing the risks that arise in their areas, ensuring that daily activities align with the organization's prioritised security objectives.

This includes:
- Maintaining risk overview and insight through regular and relevant risk assessments.
- Ensuring appropriate security proportionate to risk profile.
- Maintain/ensure relevant risk insight and awareness amongst employees, consultants and contractors.
- Escalating any security risks via chain of command, that cannot be mitigated within limits.