



Security Policy Statement

GEM-HSSE-0005

Gemini's responsibility to make the Gemini wind park as secure as possible is a guiding factor of its operations. The Gemini management team will ensure that high levels of security are in place which protect its employees, contractors or any third parties that may access any of our sites, both on shore and off shore.

The Gemini management team will ensure that high levels of cyber security are in place which protects its assets and data.

Gemini's security measures will be proportionate to the assessed risk. Security measures will apply to all business assets, including people, property, information and reputation.

Tested plans and procedures will be in place to deal with security incidents and emergencies. Security incidents and emergencies will be reported through the normal incident reporting structure, so that Gemini can improve and learn from the incidents where possible.

Gemini requires contractors to manage their security, while operating at our locations. The Gemini Security practices and procedures must be adhered to and deviations from these practices and procedures must be documented and will only be accepted when it will lead to a higher or equally effective security system. Gemini accepts that implementation is a management responsibility. Top management will provide support as required to implement all aspects of this policy and related procedures.

Security operations shall be conducted in full compliance with national legal requirements and international standards. Security shall be addressed in the same way as any other critical activity in the proposal, planning implementation and discontinuation stages of business operations. Armed security shall not be used unless it is a legal or government requirement or if there is no acceptable alternative to manage the risk.

Programs will be conducted to develop security awareness and responsibility amongst our staff, contractors and visitors. All incidents, including security breaches and irregularities shall be reported, investigated and recorded.

Security measures shall be reviewed periodically, and lessons learned, new legislation and regulations and international best practices will be taken into account.