SEMBCORP GREEN INFRA LIMITED

INFORMATION SECURITY POLICY

SGIL aims to promote and build an environment where all employees are aware of their individual security responsibilities and are actively engaged and committed to continually improving standards meeting requirements of Information Security, thereby ensure availability of assets for clean power generation.

SGIL shall implement and monitoring services & controls to ensure that:

- Information assets and IT/OT assets are protected against unauthorized access.
- Information will be available on a strict need-to-know basis only.
- Information is not disclosed to unauthorized people through deliberate or careless action.
- Confidentiality of information will be assured in accordance with client agreements and best practices.
- Information is protected from unauthorized modification.
- Applicable regulatory and legislative requirements are met.
- Disaster recovery plans for IT/OT assets are developed, maintained, and tested as far as practicable.
- The Executive Board has the direct responsibility for maintaining the policy and providing advice and guidance on its implementation.
- Information security training is provided to all users.
- All breaches of information security, actual or suspected, will be reported and investigated.
- All Department Heads are directly responsible for implementing the policy within their business areas/ departments, and for adherence to their staff.
- A culture of compliance towards information security is advocated and promoted.
- Communication of the policy.