I.T.& Physical Security Policy

Ref No:	ATEC-PLY-017		
Owner:	ATEC M.D.		
Date:	01/01/2022		
Issue No:	002	Sheet No:	1 of 2

This Policy sets out the Atec strategic commitment to information security management. It is the policy of our organisation and should ensure the confidentiality, integrity and availability of information owned by both the organisation and clients is maintained to:

- Ensure continued safety and quality of service is as agreed and expected
- Meets all contractual, legal, and regulatory obligations
- Meet the needs and expectations of other interested parties, as per the MSM

Information and facility security management shall be treated as an integral part of management activities and will be pursued in the same manner and with the same vigour as other managerial objectives.

The M.D. and board of Directors are committed to:

- Taking appropriate action to ensure the confidentiality and integrity of Atec and customer owned information, held by, and managed by Atec
- Documenting, implementing, and maintaining business continuity plans to ensure the availability of information and information systems during times of disruption
- Treating information security as a business-critical issue
- Ensuring that legislative, regulatory, and contractual requirements are met
- Protecting and respecting the intellectual property rights of Atec and other interested parties
- Creating an I.T. and physical security positive culture within Atec
- Establishing and maintaining an effective Information Security communication Forum
- Ensuring information security risks are managed to an acceptable level
- Identifying and implementing controls for information assets that are proportionate to levels of risk
- Communicating this Policy and supporting procedures to all employees, customers, suppliers, and other stakeholders
- Achieving individual accountability for compliance with this Policy, related policies and supporting procedures
- Ensuring any reporter of an incident is not punished or inappropriately disciplined.
- Ensuring all breaches of information security, actual or suspected, are reported, and investigated in line with published policies
- Documenting, implementing, and maintaining an information security management system (ISMS) in accordance with the best practice contained within ISO/IEC 27001
- Providing resource, training, and education to allow continued compliance and improvement

The Managing Director, with support from the board of Directors and senior management team have overall responsibility and authority to ensure that this Policy is effectively implemented and delivered. All employees, suppliers and contractors are required to play an active role in the protection of our assets and treat information security appropriately to facilitate compliance with this policy, regulations, and international standards.

Atec recognises the need for continual improvement. The information security management system will be regularly reviewed, and any changes communicated to all employees and interested parties. Atec implements a co-operative and “just” working culture, all employees share responsibility to ensure all our policies and procedures remain compliant and where any doubt exists employees and suppliers seek further guidance.

Managing Director