

Information Security Policy



1. Purpose



Consistent information security risk management is important for Aspen Medical Pty Ltd (Aspen Medical), its customers and stakeholders. This policy demonstrates Aspen Medical’s commitment to information security and communicates our vision of information security.

2. We commit to:

- Managing information assets in an accountable and coordinated manner in accordance with legislative and contractual requirements and principles of good governance.
- Protecting the integrity of all information disseminated, produced, managed or stored.
- Handling information, whether Aspen Medical or customer owned, through sound information security procedures in order to protect all information assets for internal, external, deliberate or accidental threats.
- Drive information security through risk based information security principles by implementing an Information Security Management System (ISMS) aligned to ISO / IEC 27001: 2013.

3. We will achieve this by living our information security principles:

Information security principles	
	<p>TRUSTWORTHY</p> <ul style="list-style-type: none"> • Embedding a culture of accountability and responsibility for the confidentiality, integrity, availability, safety and reliability of Aspen Medical’s information assets and systems • Enabling our people to take accountability for their use of information in their day-to-day role • Integrating information security risk management principles into our planning and decision-making.
	<p>TRANSPARENT</p> <ul style="list-style-type: none"> • Engaging with the business to garner feedback on our ISMS and cyber security program. • Providing engaging and appropriate information security training across Aspen Medical to ensure an understanding of the requirements of Aspen Medical’s approach to information security. • Providing clear and direct guidance on our expectations for the protection of all information, including internal, third party, personal and electronic data.

Information security principles	
	<p>PRIVATE</p> <ul style="list-style-type: none"> • Understanding the root causes of cyber security events and incidents without allocating blame or assigning punishment. • Understanding our cyber security objectives and legislative and contractual environment to ensure it is accurately represented within our information security policy framework. • Empowering our people to take responsibility in our cyber secure culture and report any concerns or risky behaviours they witness.
	<p>VALUED</p> <ul style="list-style-type: none"> • Proactively measuring our ISMS to enable reporting of the right information to the right people • Critically reviewing our ISMS to find positive ways of continually improving and developing it • Creating innovative ways of communicating our commitment and leadership in information security within our community and industry.

4. Accountability and responsibility

- Aspen Medical’s Board is accountable for ensuring sufficient resourcing, management and monitoring of the ISMS.
- The CEO is responsible for leading the implementation and compliance to the ISMS, including communicating Aspen Medical’s vision of information security and its importance.
- All executives, managers, employees and contractors must adhere to this policy and act in a manner that continually promotes a cyber-secure culture and the management of information security risk.