Acumentis
DECISION CERTAINTY

ABN: 50 102 320 329

Information Security Policy

1 Purpose

Information Security is critical to ensure the resilience and ongoing success of Acumentis. It has strategic implications for Acumentis and represents an integral part of Acumentis objectives and processes.

This policy mandates:

- Confidentiality – to uphold authorised restrictions on access to and disclosure of information including personal or proprietary information.
- Integrity – to protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
- Availability – to provide authorised users with timely and reliable access to information and services.
- Compliance – to comply with all applicable legislation, regulations, policies and contractual obligations requiring information to be available, safeguarded or lawfully used.

Defined Acumentis information security objectives to meet the above core requirements are to:

- Protect systems and information by safeguarding its confidentiality, integrity and availability;
- Establish effective information security governance within Acumentis;
- Maintain an appropriate level of staff and contractor awareness, knowledge and skills to minimise the occurrence and severity of information security incidents;
- Ensure Acumentis can continue to operate and rapidly recover its business operations in the event of a detrimental information security incident;

2 Scope

The Information Security Policy applies to Acumentis information, as well as to users of that information including employees, contractors, volunteers, and external parties.

This Acumentis Policy is aligned with the International and Australian standards AS/NZS ISO/IEC 27001:2013 and AS/NZS ISO/IEC 27002:2013. This alignment ensures that Acumentis addresses Information Security Management in a consistent way.

3 Roles and Responsibilities

Roles	Responsibilities
Chief Executive Officer (CEO)	Oversee this policy.
Chief Information Officer (CIO)	Review and approve this policy. The provision and implementation of supporting systems, applications and processes that give effect to this policy. The establishment and support of monitoring and compliance systems and processes to ensure that the supporting mechanisms are functioning effectively.
Employee, Contactors and Third Parties	Responsible for compliance with this policy, and any supporting policies, standards and procedures.
All Personnel	Reporting security incidents and any identified weaknesses.

4 Executive Support

The executive management of Acumentis supports the realisation of a thorough Information Security programme and welcomes the implementation of new, and the optimisation of, existing Information Security policies and procedures. It is the task of every management level in Acumentis to ensure a high level of security in order to support and protect Acumentis information assets and that of Acumentis business partners.

Information Security is not, however, the sole responsibility of management. All Acumentis employees, contractors and collaborators are responsible for Information Security in their respective fields.

The Information Security Policy reflects the emphasis and commitment placed on Information Security by Acumentis.

5 Security Policy

It is the policy of Acumentis that:

- Information in all forms must be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. Information may be written, spoken, recorded electronically or printed. This protection includes an appropriate level of security over the equipment, processes and software used to process, store, and transmit information.
- Establish effective information security governance within Acumentis to manage and continuously improve its Information Security posture.
- We adopt a risk-based approach, in line with its IT Risk Management Framework, to address potential gaps in its security controls. The controls selected are commensurate with the level of risk to be addressed.
- All personnel must participate in information security training when hired and at least annually.
- All personnel are responsible and accountable for their own actions in relation to this policy including all information security policies, standards and guidelines referenced in this policy and the Acumentis ISMS.
- Staff in leading roles must ensure their team members are aware of and perform their role and responsibilities in line with Acumentis information security policies, procedures and standards.
- All personnel who become aware of any potential or actual information security incident or breach must inform their line manager or appropriate senior staff immediately.
- Staff in leading roles are responsible for the regular review and treatment of information security threats and risks to the organisation.
- The use of Acumentis IT resources is not to be considered by staff to be private. Acumentis carries out ongoing monitoring and auditing of IT resource usage.
- Demonstrate compliance to external entities (customers, regulation bodies, partners) by regularly auditing security practices.
- Processes are implemented to ensure information security practices are continuously reviewed and improved to protect Acumentis from ever-evolving threats.