Information Security Management System (ISMS) Policy

The Managing Director, Board of Directors, Senior Management Team and all employees are committed to an effective and continual improvement of the Information Security Management System (ISMS) in compliance with ISO 27001:2013. To fulfil this policy, the ISMS will be certified by a UKAS accredited provider. This policy will be made available to Interested Parties, where required.

Objectives

- Provide assurance within the company and to our customers, partners and interested parties that the availability, integrity and confidentiality of their information will be maintained adequately
- Manages information security risks to all company and customer assets
- Protects the company's ongoing ability to meet contracted commitments
- Bases information security decisions and investments on risk assessment of relevant assets considering Confidentiality, Integrity and Availability (CIA)
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities

Responsibility for upholding this policy is company-wide under the authority of the Managing Director who encourages the personal commitment of all staff to address information security as part of their skills. The Information security Management System high-level objectives are reviewed and updated at least annually

To fulfil these objectives, the ISMS will:

- Prevent against unauthorized access by implementing an Access Control policy, with adequate physical and digital protections. Access violations will be measured to ensure effectiveness.
- Ensure the availability of internal and external services provided to Aculab staff and customers. The Aculab Cloud Service Level Agreement (SLA) and elements of the IT network will be measured to ensure effectiveness.
- Ensure the Confidentiality, Integrity and Availability (CIA) of Aculab's network and systems. Regular scanning of networks under the ISMS will be measured to ensure effectiveness.
- Ensure the integrity of Aculab's backup data and the ability to meet the business continuity plan. Regular restores will be performed and measured to ensure effectiveness.
- Ensure all staff are aware of Aculab's information security processes and policies. Regular training will be given to staff, and security awareness embedded into the company culture. Security weakness, events and incidents, along with awareness questionnaire results will be recorded and measured to ensure effectiveness.

APPROVED: *Alan Pound* **AP**
MANAGING DIRECTOR

REVIEWED: *Judith Charman* **JC**
FINANCE DIRECTOR

REVIEWED: *Ladan Ravary* **LD**
SPEECH TECHNOLOGIES DIRECTOR