Information Security Policy

We will establish, maintain and continually improve an ISMS (information security management system) to manage the risks affecting information belonging to our organization and relevant interested parties. We aim to protect that information from all threats (whether internal or external, deliberate or accidental), and safeguard its confidentiality, integrity, and availability. Specifically, we will ensure that:

* Business requirements for the availability of information and information systems are met.
* Information will be protected against unauthorised access.
* Confidentiality of information will be assured, by protection from unauthorised disclosure, theft, or intelligible interruption.
* Integrity of information (its accuracy and completeness) will be maintained by protecting against unauthorised modification.
* Regulatory and legislative requirements will be met.
* Business Continuity plans will be produced, maintained, and tested, to ensure that information and vital services remain available in the face of adverse events.
* All employees and relevant contractors will be made aware of key information security matters.
* All breaches of information security will be reported to the ICT Manager and investigated appropriately.
* A suitable program of independent review is implemented to identify any weaknesses in the implementation of technical security controls on classified assets.
* Our ISMS is established and maintained in compliance with the ISO 27001 standard.

While the ICT Manager and team administer our ISMS, everyone working for our organisation has a role to play and is required to comply with this Policy.

#### Jane Doe

Jane Doe

CEO

(Date)

This sample policy is based on one of many included in Qudos ISO 27001 InfoSec Toolkit.

Available in Qudos3 IMS software.



Contact [info@qudos-software.com](mailto:info@qudos-software.com) for details.