Quintessa Information Security Management System

Information Security Policy

Owner: Managing Director
Document Id: QPUB-ISMS-InformationSecurityPolicy
Version: 3.2
Review Frequency: At least every 12 months
Last reviewed: 18/11/19

Document History

Version	Date	Notes
1.0	6 Jun 2014	Produced by DPH and AP
2.0	9 May 2017	Extensive revision by AP
2.1	4 Sep 2017	Minor formatting changes by RHL
3.0	16 Sep 2018	Revision by SJB and RHL and review by AP
3.1	14 Nov 2018	Revision by SJB reviewed by RHL
3.2	18 Nov 2019	Revision by SJB reviewed by RHL

The goal of Quintessa's Information Security Policy is to protect the information assets belonging to the Company and/or entrusted to it by third parties against all internal, external, deliberate or accidental threats by ensuring all information is held and maintained in a secure and controlled environment and in compliance with all contractual and legal/regulatory requirements.

The Company's information assets are assessed using a risk assessment methodology, which is used for setting objectives for the Information Security Management System (ISMS). Risks are evaluated according to their severity and probability of occurrence. If a risk is deemed significant, its mitigation automatically becomes an information security objective.

The ISMS comprises a set of controls, including processes, procedures, organisational structures, and software and hardware functions that conform to the ISO 27001:2013 standard and the Cyber Essentials Plus Scheme. These controls are established, implemented and monitored to ensure the specific security objectives of the Company are met and all necessary security approvals and accreditations are maintained through working with employees, clients and other bodies. The Company has a commitment to review these controls through audits and, where necessary, to implement changes to ensure the continuing improvement of the system.

The Information Security Coordinator is responsible for maintaining the ISMS and providing on-going training, support and advice during its implementation. All employees are directly responsible for implementing the requirements and responsibilities of the ISMS.

This Policy is subject to annual management review and is updated as necessary. All changes to this Policy, and to the ISMS in general, must be approved by the Managing Director.