Quality and Information Security Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	CKT02001
VERSION	12
DATED	03 August 2020
DOCUMENT AUTHOR	Ken Holmes
DOCUMENT OWNER	Product Manager

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	2 Jul 2014	Ken Holmes	First version.
1.1	31 Oct 2014	Ken Holmes	Minor updates to wording.
2	16 Jan 2015	Ken Holmes	Reformatting based on recommendations from internal audit of 14 Jan 2015.
3	28 Jan 2015	Ken Holmes	Change to scope statement as a result of ISO/IEC 27001:2013 Stage One review on 27 Jan 2015.
4	20 Feb 2015	Ken Holmes	Reference to monthly and annual management reviews added to section 2.10 as result of external audit on 17 Feb 2015.
5	20 Oct 2015	Ken Holmes	Updated to cover ISO9001 requirements as part of combined management system.
6	31 Oct 2015	Ken Holmes	Made more concise. Commitment emphasised as result of ISO9001:2015 stage one audit on 29 Oct 2015.
7	23 Nov 2015	Ken Holmes	Minor changes to wording from internal audit of 23 Nov 2015.
8	26 Jul 2016	Ken Holmes	Increased mention of information security.
9	30 May 2018	Ken Holmes	Changed to reflect renaming of company from Public IT Limited to CertiKit Limited.
10	10 Jul 2019	Ken Holmes	Document owner changed.
11	8 June 2020	Mark Clifton	Document put into new CertiKit brand.
12	3 Aug 2020	Ken Holmes	Correction to ISO9001 scope statement.

Approval

NAME	POSITION	SIGNATURE	DATE
Ken Holmes	Managing Director	K. Holmes	3 Aug 2020

Contents

1 Introduction

The management of CertiKit Limited strongly believe that the use of a structured management system not only makes sense today but will become increasingly beneficial as the company grows.

1.1 Scope

For the purposes of certification to the ISO 9001:2015 standard, the boundaries of the management system are defined as follows:

The provision of document toolkit and related management services: email support, update and consultancy.

For the purposes of certification to the ISO/IEC 27001:2013 standard, the boundaries of the management system are defined as follows:

The management of information security in the provision of document toolkits and related services provided by CertiKit Limited to its customers in accordance with its Statement of Applicability.

2 Policy

The top management of CertiKit is committed to ensuring that its products are designed and developed to meet our customers' requirements in as many ways as possible. We will ensure that we use the various methods at our disposal to capture and understand our customers' requirements as fully as we can. This will often be via pre-sales enquiries, post-sales support questions and via our annual customer feedback survey.

The Managing Director of CertiKit Limited is committed to the success of the management system and this will be demonstrated through this Quality and Information Security Policy and the provision of appropriate resources to provide and develop the management system and associated controls.

The Managing Director will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that quality and information security objectives are being met and quality and information security issues are identified through the audit programme and management processes.

An annual cycle will be used for the setting of quality and information security objectives, to coincide with the business planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements.

The top management of CertiKit is committed to a policy of continual improvement. Ideas for improvements may be obtained from any source including business advisors, customers, suppliers, and auditors.

Risk management will take place at several levels within the management system, including:

- Management planning – risks to the achievement of objectives
- Business process risk assessments
- Information security risk assessments
- As part of the design and transition of new or changed services

High level risk assessments will be reviewed on at least an annual basis or upon significant change to the business or service provision.

CertiKit will ensure that all staff involved in the business and in information security are competent based on appropriate education, training, skills, and experience.