

douglas stafford®

When performance is *everything*.

INFORMATION SECURITY POLICY STATEMENT

All information, regardless of its origin, form or format, which is created or used in support of business activities, is defined as Douglas Stafford corporate information.

Corporate information is a company asset and must be protected from its creation, through its useful life and authorised disposal. It should be maintained in a secure, accurate, reliable manner and be readily available for authorised use.

Information will be classified based on its sensitivity, legal, and retention requirements, and types of access required by employees and other authorised personnel.

Information security is the protection of data against accidental or malicious disclosure, modification or destruction. Information will be protected based on its value, confidentiality and / or sensitivity to the company, and the risk of loss or compromise. At a minimum, information will be update-protected so that only authorised individuals can modify or erase the information

The Information Security program described in the Best Practice Management System manual has been specifically designed to meet the requirements of ISO 27001:2005 (as well as ISO9001:2008) and to provide the framework to allow accomplishment of our Information Security objectives and goals.

The company has appointed a senior full time member of staff as the Chief Information Security Officer (CISO) and he has Board approval to issue, maintain, implement and withdraw policies and procedures as necessary. He is also the focal point for all staff, contractors and subcontractors who have any questions / queries regarding the Information Security Management System.

Douglas Stafford's board of directors have committed to the Quality Management System

This ISMS Security Policy is available to the public at our website: www.douglasstafford.co.uk

Considered 'uncontrolled' when printed