Secure Agility

Information Security and Business Continuity Policy Statement

Document version: 1.01

Published: June 2021

Information Security and Business Continuity Policy Statement

As a modern, forward-looking business, Secure Agility recognises at senior levels the need to ensure that its business operates securely and without interruption for the benefit of its customers and other stakeholders.

In order to provide such a level of assured and continuous operation, Secure Agility has implemented an Integrated Management System (IMS) in line with the International Standards ISO/IEC 27001 for Information Security, and ISO 22301 for Business Continuity.

Secure Agility's Directors are committed to the maintenance of the Information Security and Business Continuity capabilities, which identify how security, incident, crisis and continuity management will be governed, delivered, tested, maintained and improved.

This will ensure that the levels of organisational resilience developed across Secure Agility will continue to meet the needs of the Company and its obligations to its clients. The Strategic Recovery Priorities and their associated recovery parameters define the scope of the Policy. The scope applies to services provided by Secure Agility to its clients including the provision of managed hosting, cloud computing, reseller services, managed services, consulting, project management, service management and data centre co-location services and talent management.

The purpose of this Policy is to ensure that Secure Agility continues to meet the expectations and requirements of its clients and partners. To achieve this analysis, planning, training and rehearsing takes place so that risks to information security and service provision can be identified and treated to reduce likelihood and impact. Recognising residual risks may remain, recovery strategies are in place to limit disruption, should such risks occur, by enabling services to be recovered within acceptable timeframes and to predetermined service levels.

Top management will ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that information security and business continuity objectives are being met and relevant issues are identified through an audit programme and management processes.

This policy will be reviewed for continuing suitability at least annually or when significant changes occur, and made available to all employees, stakeholders and interested parties as approved by management.