Information Security Policy

1. Introduction

1.1. The Information Security Policy recognises that during the course of our operations, we are required to preserve the confidentiality, integrity and availability of information that we generate or are entrusted with by our suppliers, contractors, clients and customers.

1.2. This policy applies to Salisbury Workspace Services Limited's Information Security Management System (ISMS), hereinafter Salisbury.

1.3. Salisbury Workspace Services Limited forms part of Salisbury Group.

2. Scope

2.1. Salisbury Group has implemented an Information Security Management System (ISMS) in accordance with the international standard ISO/IEC 27001. This policy outlines how Salisbury will protect all organisational assets from all relevant threats, whether internal or external, deliberate or accidental.

3. Procedures

3.1. We will achieve the above by:

3.1.1. Ensuring that information is made available with minimal disruption to staff and customers as required by the business.

3.1.2. The integrity of this information is maintained.

3.1.3. The confidentiality of information is preserved.

3.1.4. Regulatory, legislative and other applicable requirements related to information security are met.

3.1.5. Appropriate information security objectives are defined and, where practicable, measured.

3.1.6. Appropriate business continuity arrangements are in place to counteract interruptions to business activities and these take information security into account.

3.1.7. Appropriate Information security education, awareness and training is available to staff and relevant others working on behalf of the company.

3.1.8. Breaches of information security (actual or suspected) are reported and investigated through the appropriate processes.

3.1.9. Appropriate access control is maintained, and information is protected against unauthorised access.

3.1.10. Continual improvement of the ISMS is made as and when is appropriate.

4. Responsibilities and review procedure

4.1. The Commercial and Finance Director has been appointed as the senior executive with responsibility for information security.

4.2. The senior executive will work with the Director of Security and other colleagues as necessary to review this policy as part of the defined management review process.

4.3. Any changes made to this policy will be communicated to all employees as required.

5. Date of approval

5.1. The Information Security Policy was approved by the Group MD on the date stated below.

5.2. A current version of this document is available to all members of staff on the corporate intranet and publicly available on the company website. It will also be provided to interested parties on request.

Date: 01/03/2022