



Information Security & Risk ISO 27001:2013

Information Security Policy Statement

This policy statement outlines the Downing Partners' endorsement and intent for Information Security Management (ISM) within Downing. Its purpose is to communicate our ISM expectations to all those delivering services upon our behalf or working on our premises.

Some aspects of our operations, including handling personal data and having privileged access to locations, present clear information security requirements, however it is expected that we treat all our client and internal hard copy and electronic information in a secure manner, throughout all our processes.

Our overall ISM objective is to protect the organisation from incidents that might have an adverse effect on the people we work with, our business operations and our professional standing. Information Security issues can include Confidentiality (people obtaining or disclosing information inappropriately), Integrity (information being altered or erroneously validated, whether deliberate or accidental) and Availability (information not being accessible when it is required).

Many types of incidents can pose a threat to our effective use of information. This includes performance, consistency, reliability, accuracy and timeliness. More detailed ISM objectives and monitoring will be defined separately to this policy, either within a stand-alone document or within management review.

Our information security management system is part of our ISM and using this framework, we will assess and manage ISM risk. We shall also understand and comply with any applicable ISM or related legal/regulatory requirements.

This statement has been prepared to demonstrate a commitment to continual improvement within our Information Security Management System. This message shall be communicated and understood throughout Downing and it is expected that all persons performing work on our behalf share this commitment to these values.

It is the responsibility of all our staff, regardless of grade, to become familiar with our security processes and to comply with all information security and privacy policies and the procedures that underpin them.

This Policy Statement shall be made available to the public, upon request, and shall be communicated and adhered to by all employees, temporary staff, contractors and visitors who enter any of our work sites.

This policy has been approved & authorised by:

Name: JAMES WEAVER
Position: COO
Date: 01.08.2023
Signature:

