

# Information Security Policy

## 1. Scope

This policy applies to all Babington colleagues, agents, contractors, and anyone given access to any Babington system, including systems operated by third-parties.

## 2. Purpose

- To communicate the Board and Executive's commitment to protecting the confidentiality, integrity, and availability of the organisations' information assets.
- To set out the strategic direction for the management of information security and privacy.
- To specify the implementation of an Information Security Management System (ISMS) and to achieve and maintain Certification of that ISMS to the ISO 27001 standard.
- To serve as the overarching policy from which the framework of policies, procedures, and records that form the ISMS derive.
- To promote a risk-based approach into the organisation's culture.
- To set out the organisations' information security and privacy objectives.

## 3. The Policy

- Department Heads are committed to ensuring all information assets held, stored, or processed, including those processed on Babington's behalf by a third party, are securely protected against unauthorised access, disclosure, alteration, or loss in accordance with legal, regulatory, and contractual obligations.
- Babington's information security and privacy management and processes are aligned with and support the aims and objectives set out in strategic business plans. Information and privacy related risks will be identified, assessed, and mitigated through risk assessments and risk treatment plans.
- The organisation's commitment to, and management of, information security and privacy is governed by the Information Security Steering Group (ISSG) which reports to the Executive and Board. The ISSG is chaired by the Chief Finance Officer and the ISSG provides overarching governance for information security and privacy and comprises management representatives from key departments. The Chief Executive Officer has delegated the role of Senior Information Risk Owner to the Chief Finance Officer. The ISSG Terms of Reference support the ISMS framework and requires periodic reviews of ISMS policies, including an annual Management Review attended by the Chief Finance Officer.

## 4. Objectives

- To demonstrate continual improvement and maintain ongoing ISO 27001 Certification by the continued evaluation and review of our effectiveness measurements and ongoing internal information security and privacy audits to identify and address areas for improvement.
- To ensure the organisation fulfils its legal, regulatory, and contractual responsibilities under Data Protection and other relevant Legislation.
- To ensure information security and privacy are embedded throughout the organisation and is taken account of in all established management frameworks, strategic aims and objectives and organisational process and practice.
- To preserve the confidentiality, integrity, and availability of all information assets. This will be achieved by:
  - Determining and documenting the processes into which information security and privacy should be integrated across all functions of the organisation.
  - Ensuring that all users who access Babington's ICT system and/or premises are aware of their security responsibilities.
  - Ensuring that all information and associated assets are accessible to authorised users when required and that information is only accessible to those authorised and to prevent unauthorised access to Babington's information, intellectual property, and information processing assets.
  - Ensuring that safeguards are in place to protect the accuracy and completeness of information and to prevent deliberate or accidental, partial, or complete, destruction or unauthorised modification of data or any other information asset.
- To ensure a risk-based approach underpins all strategic decision making and that privacy and information security issues and risks are identified, assessed, and managed as part of this decision-making process.
- To ensure the organisation implements and maintains a fully integrated records management process which meets its legal and contractual obligations and assigns responsibility for facilitating the timely disposal and/or deletion of all records.
- To ensure performance against these objectives form part of the Effectiveness Measurement monitoring by the ISSG.

## 5. Owner and Approval

The Chief Finance Officer is the owner of this document and is responsible for ensuring that this policy is reviewed in line with the review requirements of the Management Review of the ISMS.

The current version of this document is available to all colleagues on the corporate intranet. It does not contain confidential information and can be made available to relevant interested parties.

The Information Security Policy was first approved by the ISSG and is issued on a version-controlled basis under the signature of the Chief Finance Officer.

Signed by: *Thomas Smith*

Date: 27<sup>th</sup> November 2023

Tom Smith  
Chief Finance Officer and SIRO