Information Security Policy

Introduction

This policy documents Babington's commitment to information security, continual improvement and satisfying applicable information security requirements of our interested parties such as employees, customers, partners and suppliers.

Scope

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

Information Security Statement.

"Babington recognises that the security of the information entrusted to us by our employees, customers, partners and suppliers is of paramount importance, and ensures the confidentiality, integrity and availability of that information through Policies, Processes and Controls to provide our stakeholders with the assurance that their information is in safe hands".

Principles

Babington is committed to the development, implementation and maintenance of an Information Security Management System (ISMS) that:

- Defines the scope of Babington's operations subject to the ISMS;
- Provides assurance within Babington, and to our customers, partners, suppliers and other interested parties that the availability, integrity, and confidentiality of their information will be maintained appropriately;
- Manages information security risks to in-scope Babington and customer assets;
- Protects Babington's ongoing ability to meet contracted commitments through appropriate Business Continuity;
- Bases information security decisions and investments on the risk assessment of relevant assets considering integrity, availability, and confidentiality;
- Considers business and legal or regulatory requirements and contractual security obligations;
- Maintains awareness of all colleagues so that they can identify and fulfil contractual, legislative, company and Group specific security management responsibilities;
- Minimises the business impact of, and deals effectively with, security incidents;
- Ensures 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.
- Meets the requirements of any other interested parties not already specified.

Objectives

Babington aims to ensure that it has:

- A senior management team that supports the continuous review and improvement of the information security management policies and processes;
- Implemented company-wide policies and procedures that support our information security statement;
- General policies and processes for the protection of corporate information as well as employee, customer, and supplier information;
- Implemented an information security risk assessment process that assesses the harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities and controls currently in place;
- Developed and implemented a Business Continuity Plan to counteract disruptions to business activities and to protect critical business processes from the effects of major failures or disasters
- Defined physical and logical access controls to prevent unauthorised access, damage to and interference with business premises and information;
- Implemented an incident management and escalation procedure for reporting and investigating security incidents for review and action.

These policy aims are supported by the following objectives:

1) To provide assurance to customers and partners that Babington's information security controls are robust and effective;
2) To ensure awareness of information security policies is maintained for all employees, agents and contractors;
3) To continually improve the ISMS and ensure it adapts to internal and external changes;
4) To deal with all information security weaknesses and incidents effectively and address the root cause (where applicable);
5) To ensure that system access is tightly controlled and only issued on a need-to-know basis;
6) Handle client data in accordance with company policy and client expectations;
7) To demonstrate a high level of control on company IT Assets;
8) To ensure that the business remains functional during periods of unplanned interruption or threat occurrence;
9) To ensure that data can be recovered promptly in the event of loss or request for an archive by a customer;
10) To effectively manage third party suppliers who process, store, or transmit information to reduce and manage information security risks.

Information Security Defined

Information security is defined as preserving:

Information Security Policy Framework

This policy forms part of the Information Security Management System (ISMS) at Babington. This policy should be read in conjunction with all other Babington ISMS policies and procedures, which are updated as necessary to maintain an effective ISMS to meet Babington's business needs and legal obligations.

It is the responsibility of employees and contractors to read these and report any non-compliance in accordance with the Incident Reporting and Response Policy and Procedure.

Information Security Roles and Responsibilities

Information Security is the responsibility of everyone to understand and adhere to the policies, follow process(es) and report suspected or actual breaches. Specific roles and responsibilities for the running of the Information Security Management System are defined and recorded in relevant policies. Key responsibilities for specific roles are outlined below.

The Management Team:

- Ensures an Information Security Policy and supporting processes are set and maintained;
- Reviews changes to Babington's organisation and operations to assess the impact on information security;
- Promotes security requirements and issues throughout Babington;
- Maintains a continual improvement programme for Babington's information security arrangements.

The Chief Executive:

- Actively supports information security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities;
- Provides the resources needed to maintain the ISMS and support information security related activities;
- Approves the assignment of specific roles and responsibilities for information security across the organisation.

The Data Protection & Information Security Manager, supported by the Management Team:

- Coordinates information security related activities within Babington;
- Schedules, chairs and documents information security management reviews;
- Reviews and approves information security policies, methods, and processes;
- Maintains information security related policies and procedures, including annual reviews to ensure continuing suitability, adequacy, and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the information security policies and processes;
- Maintains change, control, and integrity of information security documents;
- Analyse incident reports, identifies root cause and planned improvement actions, and reports to the Directors, recommending actions where appropriate;
- Conducts risk assessments of information security assets, identifying significant threat changes and exposure of information and information processing facilities to threat;
- Organises and conducts audits and reviews of the information security policies and processes;
- Periodically reviews the organisation business continuity requirements and maintains the company's business continuity plan;
- Manages the external assessment interface for ISO27001 certification;
- Ensures that Directors and colleagues are fully aware of their obligations with respect to information security;

Colleagues:

- All Babington colleagues, agents, contractors, and anyone given access to any Babington system, including systems operated by third parties, are responsible for ensuring Babington's policies and associated requirements are complied with, within their area of responsibility and operation.

Legal and Regulatory Obligations

Babington takes its legal and regulatory obligations seriously and these requirements are record in the document "2333 Legislation, Regulation & Interested Parties and Compliance Register".

Training and Awareness

Babington has determined that it is mandatory for all staff members to complete information security and data protection training as part of their induction and as part of organisation wide annual refresher training thereafter.

Babington expects that all third parties with access to Babington information, such as sub-contractors or third-party supplier personnel also receive induction and refresher training appropriate to the nature of the information, they have access to. In line with legislative and contractual obligations and any identified information risks.

Policies are made readily and easily available to all employees and appropriate third-party users.

Continual Improvement of the Management System

Babington is committed to a process of continually improving the effectiveness of its ISMS. The ISMS Management Team is responsible for ensuring that all quality and information security related improvement plans, corrective action, and non-conformities are collated and documented appropriately. These may arise from several sources, including:

- Management reviews;
- Internal and external audits;
- Annual business improvement objectives;
- Incident reporting;
- Change management
- Financial reporting
- Resourcing reporting;
- Business continuity testing;
- Suggestions and issues raised by employees
- Client complaints and compliments;
- Supplier reviews
- Other Babington and/or Knovia Group reviews and meetings
- Day to day business activities.

Policy Compliance

Compliance Measurement

The information security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits on a periodic basis, and feedback to the policy owner. Any identified non-compliance will be investigated to understand and address the reasons for the non-compliance.

Non-compliance

Compliance with this and all other policies and procedures within the Information Security Management System is mandatory. Any colleague found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Policy Review

This policy will be reviewed by the policy owner or their nominated delegate at regular intervals, not exceeding 1 year, or when business changes warrant it as part of the continual improvement process.

The Information Security Policy has been approved by and is issued on a version-controlled basis under the signature of Babington's Chief Executive Officer.

Signed by:  Date: 11 July 2025

Jennifer Bramley

Chief Executive Officer Babington