

Sabio Group Information Security Policy



DOC A5 Document Control

Document Control

Reference:	DOC A5
Issue No:	V8.2
Version Date:	01/04/22

Confidentiality Notice

This document and the information contained therein is the property of Sabio. This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Sabio.

Sabio Group Information Security Policy

The Board and Management of Sabio Ltd, based in Sabio Global Headquarters 12th Floor, Bluefin Building, Southwark, London, UK, which is a provider of the provision of global support, managed services, unified communications, application development, hosted telephony and call centre solutions as defined in ISO 27001:2013 certificate: 682066, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets pertinent to the ISMS scope.

The Chief Executive Officer and Senior Management Team are committed to the implementation, on-going management and maintenance of the ISMS in order to ensure and support the key Information Security objectives of the business:

- Continued provision of service to clients in accordance with defined Service Level Agreements (SLA)
- Provision and maintenance of a secure Sabio internal working environment inclusive of access portals provided to clients
- Protection of all Sabio data and assets, including client data, to prevent unauthorised access, and restriction or prevention of improper use of assets
- Maintain supply chain support in accordance with the objectives of the ISMS and visibility of key performance indicators
- Maintenance of clear visibility and forecasting of all operational system functions, security, capacity and capabilities
- All staff and contractors undergo Information Security and GDPR Training annually

To that end Sabio is committed to:

- Reviewing and assessing the effectiveness of the risk management criteria and subsequent treatment plans

- Developing, assessing and implementing controls, measurable policies and practices in accordance with the organisation's structure, responsibilities and governance
- Ensuring that defined service level agreements and measurable services are provided to its clients to provide information security and customer satisfaction
- Ensure its supply chain support Sabio in its aims
- Implementing, maintaining and evaluating effective Business Continuity and Disaster Recovery plans relevant to the organisation and its client facing requirements
- Complying with relevant legal and regulatory requirements relevant to its ISMS
- Setting and monitoring relevant measures of effectiveness of its security arrangements
- Continually improving the effectiveness of the ISMS

Information and information security requirements will continue to be aligned with Sabio's goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

Our current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The risk assessments, Statement of Applicability and risk treatment plans identify how information-related risks are controlled. Continual risk assessments will be carried out when appropriate to review changing risks and the continued effectiveness of controls.

This policy is communicated to all staff and others working on behalf of the organisation, it is available to interested parties upon request.

All employees and contractors of Sabio are expected to comply with this policy and with the ISMS that implements this policy. All staff receive appropriate training.

The ISMS is designed to comply with ISO27001:2013 and we intend to maintain such compliance.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, "information security" is defined as:

Preserving the availability, confidentiality and integrity of physical and information assets of Sabio Group Ltd and our Customers

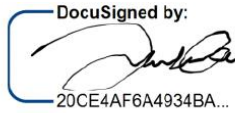
The **ISMS** is the Information Security Management System, of which this policy and other supporting and related documentation is a part, and which has been designed in accordance with the requirements of ISO27001:2013

A **SECURITY BREACH** is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the Organization.

The Chief Executive Officer (CEO) is the Owner of this document and is responsible for ensuring this policy document is reviewed.

A current version of this document is available to all members of staff, customers and publicly as appears on the Sabio website.

This information security policy was approved and is issued on a controlled basis under authority of the Chief Executive Officer (CEO).

DocuSigned by:

20CE4AF6A4934BA...

Signature:

Version	Date of Issue	Change
Issue 3.0	10/10/13	Initial issue
Issue 4.0	04/03/14	Rewrite to meet requirements of standard.
Issue 5.0	06/04/15	To reflect ISO 27001:2013 requirements.
Issue 6.0	09/11/18	Updated following Management Review
Issue 7.0	08/11/19	No changes but reviewed as part of annual review process
Issue 8.0	25/06/20	Update with change of CEO
Issue 8.1	23/06/21	ISMS review update
Issue 8.2	01/04/22	ISMS review update

info@sabiogroup.com

www.sabiogroup.com

 [@sabiosense](https://twitter.com/sabiosense)



 **SABIO**