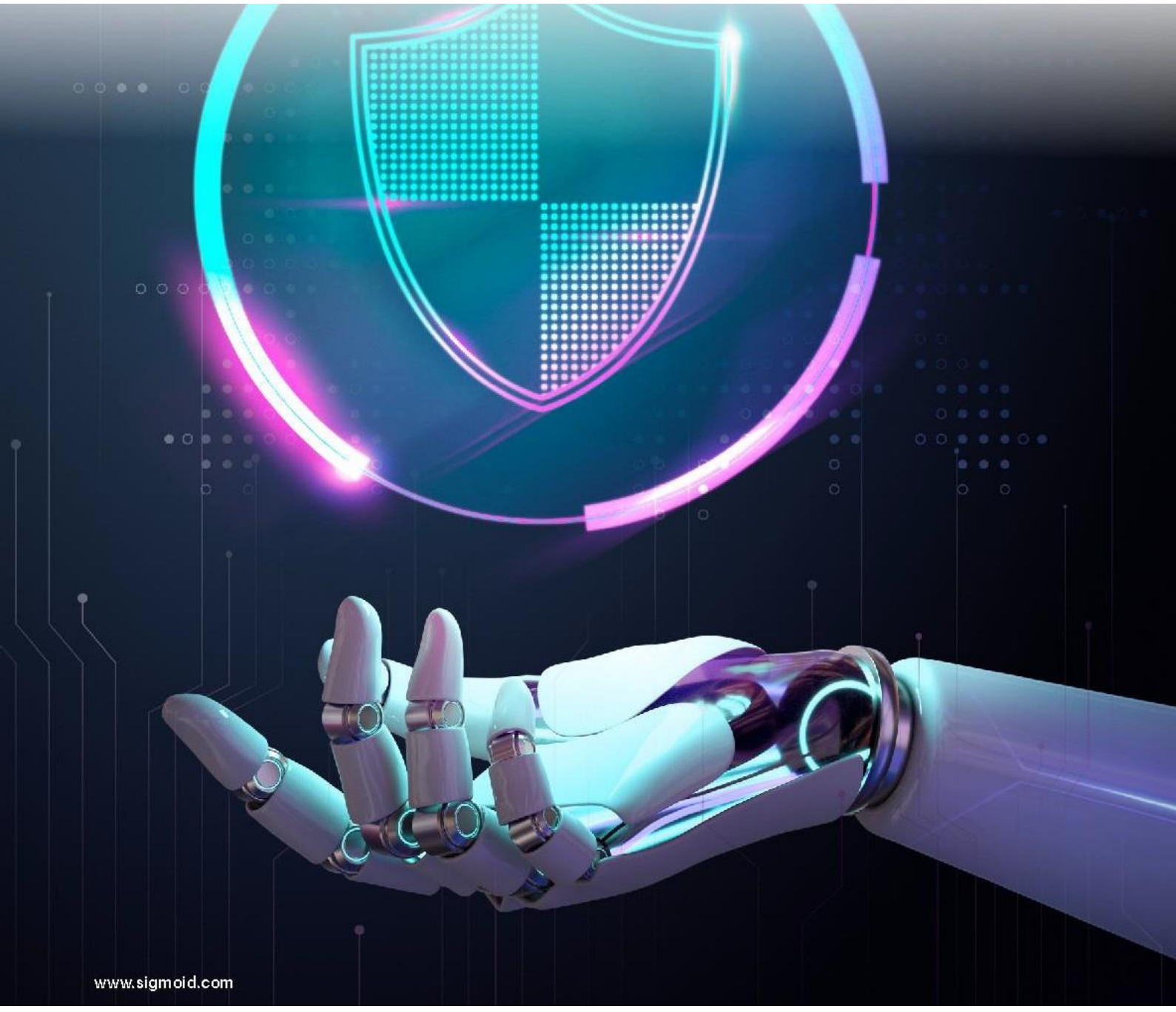
Policy

SIGMOID

# Information Security Policy



# Information Security Policy

## Sigmoid Analytics

Tower-2, SJR I Park 2nd Floor, Rd Number 9, Whitefield,
EPIP Zone, Bengaluru, Karnataka 560066

## Table of Content:

## Document Summary

| | |
|---|---|
| **Document Reference ID** | S-IS-POL-ISP |
| **Version Number** | 3.2 |
| **Document Type** | Policy |
| **Author** | E Narasimhan |
| **Reviewed By** | Information Security Team |
| **Approved By** | Anil Sharma – Director Information Security |
| **Release Date** | 20-April-2023 |
| **Next Review Date** | 04-Jun-2025 |

## Revision History

| Version | Date | Author | Significant Changes |
|---|---|---|---|
| 1.0 | 23-July-2020 | E Narasimhan | Introduction of Policy |
| 2.0 | 20-Aug-2021 | E Narasimhan | Updation of the policy based on ISMS requirements |
| 3.0 | 20-April-2023 | Naveen Kumar S | Annual document review completed |
| 3.1 | 04-June-2023 | Naveen Kumar S | Annual document review completed |
| 3.2 | 04-June-2024 | Naveen Kumar S | Annual document review completed |

# 1. PURPOSE

This document defines Sigmoid's position on information security. The objective of this policy is to describe the security requirements for information assets belonging to Sigmoid used across the Company. The policy is applicable across the company and subject to amendment at any time depending upon the changes in business requirements or environment with requisite approvals.

# 2. SCOPE

The scope of this document applies to all employees, third parties, and all information assets owned and/or handled by Sigmoid irrespective of the data location or the type of device or system it resides on. This includes electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

# 3. POLICY

## 3.1 POLICY DEFINITION

Sigmoid management is committed to protect, improve, and account for all information and information systems. Sigmoid management shall ensure that:

a) The information assets are subjected to periodic Risk assessment,
b) An effective incident response management and response is provided,
c) Awareness training is provided to stakeholders,
d) Critical business processes and information are protected by an effective Business continuity management mechanism
e) Appropriate legal and regulatory requirements are complied with.

## 3.2 ISMS OBJECTIVES

Sigmoid aims to protect its business information from threats identified, either internal or external by enforcing and measuring appropriate controls. Sigmoid management shall adhere to the ISMS Information Security Policy and established underlying detailed Policies & Procedures. The Information Security Management shall also conduct periodic review meetings for the continual improvement of information security. Sigmoid have identified the following objectives for the Information Security Management System:

- To provide a safe working environment for human resources
- To establish a robust information security framework and ensuring its alignment to key business objectives.
- To establish robust Sigmoid information security management framework, by performing threat assessment and identification of related risks associated with information assets.
- To comply with the statutory, regulatory, and contractual requirements as applicable.
- To implement mechanisms to ensure that information security breaches are reported and appropriately investigated followed by adequate actions.
- To create and maintain awareness of information security across the organization.
- To establish, implement, maintain, and continually improve information security management system.

## 3.3 RISK ASSESSMENT

The purpose of risk assessment is to evaluate the vulnerabilities and threats to the organization's information assets. The scope is defined by the Information Security Management System (ISMS). The assessment could be qualitative or quantitative.

The frequency of the risk assessment would be once every year, unless a shorter frequency required, as decided by the Security Steering Committee.

However, when there is an infrastructure change, any interested party requirements, any issues, or any addition in the organization, the risk assessment could be performed additionally on the informational asset.

## 3.4 APPLICATION ENGINEERING AND DEVELOPMENT

Sigmoid ensures the engineers are trained in industry-leading secure coding standards and guidelines to ensure products are developed with security considerations from the initial stages of programming.

All software deployment goes through staged deployments — first to a staging environment, where an automated continuous integration (CI) platform runs a host of application tests for errors and vulnerabilities. On successful completion of the same, the code is deployed to production by an authorized member of the DevOps team.

Further, an active bug-bounty program is also in place, through which white-hat hackers are invited to disclose active vulnerabilities in the application and are rewarded for verified claims.

### 3.5 APPLICATION-LEVEL SECURITY

All the systems are deployed through Azure's hosting services, which have leveraged their industry-grade best practices to protect the API endpoints. The infrastructure for databases and application servers is managed and maintained by the cloud service providers.

At the forefront, requests made to the API endpoints through Azure CloudFront infrastructure (content delivery network). Through this, Sigmoid has deployed a Web Application Firewall (WAF), which allows to identify and isolate malicious actors through automated rules. These include, but are not limited to:

- IP whitelisting/blacklisting
- Request headers-based whitelisting/blacklisting
- IP based throttling
- DDoS protection

In addition, another layer of firewall is deployed at the server instance level to ensure that only certain ports are available for network communication.

Further, at the application code level, fine-grained controls through API security credentials and authorization roles are in place to provide effective safeguards for data isolation and request throttling.

All API endpoints offer SSL encryption using SHA-256 and 128-bit keys.

A periodic 3rd party code reviews and auditing of all our production code is in place. This is done using the industry standard software. The Open Web Application Security Project (OWASP) backed tool, is also used, to provide a continuous assessment of application code to safeguard against vulnerabilities.

### 3.6 ACCESS RESTRICTIONS

All individual accesses are configured using Azure Individual Access Management (IAM) console. This allows to ensure that precise access controls are in place to limit access based on:

- Type of infrastructure resource
- Level of access to infrastructure – read/write
- Region of deployment of infrastructure – , India, US.

All accesses and actions are logged on a real-time basis. Audits are performed at randomized intervals within every 45-60 days.

Each individual's IAM access is further protected using a 2nd Factor Authentication (2FA) mechanism, which ensures that in the unlikely event that someone's access credentials are compromised, a malicious entity can't gain access without having physical control of the individual's phone or laptop.

Developer's and authorized personnel can still access application servers for general housekeeping and DevOps purposes. These accesses are strictly governed within the following constraints:

- For server access, only a public key based SSH access is granted. No usernames or passwords are issued. Each key in turn is mandated to have the most restrictive access grants within the local machine, such that, only the developer's account on the machine can access/read the key.
- SSH to the servers is only possible from a list of whitelisted IP addresses. These IP addresses are those assigned to the gateway setup at the office.
- All access to the transactional data in the database is handled through applications, where credentials are issued subject to clearly defined Access Control Lists (ACL). These accesses are all logged and audited at randomized intervals within every 45-60 days.

### 3.7 OPERATIONAL SECURITY

Sigmoid understands that formal procedures, controls, and well-defined responsibilities need to be in place to ensure continued data security and integrity.

Operational security starts right from recruiting an engineer to training and auditing their work products. The recruitment process includes standard background verification checks (including verification of academic records) on all new recruits. All employees are provided with adequate training about the information security policies of the company and are required to sign that they have read and understood the company's security-related policies. Confidential information about the company is available for access only to select authorized Sigmoid employees.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organizational security policies.

No third parties or contractors manage software or information facilities, and no development activity is outsourced. All employee information systems are authorized by the management before they are installed or used.

To test the resilience of the hosted application, the company employs an external security consultant and additional ethical hackers who perform penetration tests. Any test which has the potential of disrupting the platform's stability are always performed on an architecturally equivalent copy of the system with obfuscated customer data present.

### 3.8 PHYSICAL SECURITY

The Sigmoid development centre in Bangalore, India is under 24x7 security protection, at both premises level and floor level to ensure only authorized individuals have access to the building and the Sigmoid office. At the premises level, the building's perimeter is secured by barriers and guards. At the floor level, security cameras are installed to track movement. Access to the workspace is controlled with biometric readers, which are present to authorize individuals. Configuration of the biometric readers to grant access is controlled through a secured dashboard, which can only be accessed by the HR team.

Fire alarms and water sprinklers are in place to detect and mitigate damage in the unlikely event of a fire. Regular fire drills are also conducted by the premises management team to educate employees about emergency evacuation procedures. The office is provided with 24x7 power supply, supported by an alternative uninterrupted power supply system to ensure smooth functioning in the event of power failure.

Sigmoid hosts its application and data in industry-leading Azure, whose data centres have been thoroughly tested for security, availability, and business continuity.

### 3.9 ANTI-VIRUS AND ANTI-MALWARE PROTECTION

Malware protection and anti- virus controls are distinct elements of the IS program standards. The standards require the installation, use, and maintenance of anti-virus and anti-malware software to detect malicious code on hardware, software, networks, and/or mobile devices/ Testing and employment of such software is required and virus definitions are updated as they become available. Industry standard End-Point Protection system is in place which performs regular scanning.

### 3.10 DATA PROTECTION

Effective data protection management reduces the risk of Sigmoid from incidents related to information theft, loss, or disclosure. Encryption of data at rest and transit are made mandatory.

### 3.11 CUSTOMER INFORMATION

Sigmoid takes the protection and security of its customer's data very seriously. Sigmoid manages the security of its application and customers' data. However, provisioning and access management of individual accounts is at the discretion of individual business owners.

Our products collect limited information about customers - name, email address and phone - which are retained for account creation. No payment related information, in any part, either travels or resides on our systems.

Application logs are maintained for a duration of 15 days.

All our transaction data is backed up in 2 ways:

- A continuous backup is maintained in different data centres to support a system failover if it were to occur in the primary data centre. Should an unlikely catastrophe occur in one of the data centres, businesses would lose only five minutes of data.

- We maintain snapshots of all our data every 24 hrs. In the event of a catastrophic outage, the system's state can be recovered to the last state within a short duration.

### 3.12 DATA DELETION

When a business terminates its engagement with Sigmoid, on request all associated data is destroyed within 14 business days. If no request is made, the data is archived to a secured storage. Sigmoid products also offer data export options which businesses can use if they want a backup of their data before deletion.

### 3.13 IMPLEMENTATION EFFECTIVENESS

Sigmoid shall develop appropriate and measurable metrics to measure the effectiveness of the ISMS implementation. The areas of improvement shall be noted and actioned upon.

### 3.14 POLICY DISTRIBUTION

This Policy shall be made available only to employees and the contract staff of Sigmoid.

However, the policy may be shared with External Auditors / Consultants, Business partners, Customers, Contractors, and regulatory bodies after signing NDAs (Non-Disclosure Agreements).

### 3.15 POLICY DEVELOPMENT, MAINTENANCE AND REVIEW

CISO is primarily responsible for developing, maintaining and reviewing the Information Security Policy in coordination with the Security Steering Committee (SSC). Sigmoid Information Security Policy shall be reviewed once in a year. The Information Security Policy shall also be considered for review when there is a major change in the Business processes/physical locations and associated IT infrastructure.

## 4. ENFORCEMENT

Sigmoid expects all employees to comply with this policy and any related policy, standards, processes, procedures and guidelines. Failure and/or refusal to abide by this policy may be deemed as violations. Compliance with the policies will be a matter for periodic review by the Information security officer / Information Security Team. Any employee found to have violated this policy may be subject to disciplinary action, as deemed appropriate by the policies of management and Human Resources.

- **Monitoring:** the company employs appropriate technology solutions to monitor policy/ procedure compliance.
- **Self-Assessment:** Managers and Department Heads are required to conduct self-assessment within their areas of control to verify compliance to this policy/ procedure.
- **Security Audits:** Internal Audit may assess the implementation of and compliance with this policy/ procedure as part of its audit program.

## Special Circumstances and Exceptions

All exceptions to this policy/ procedure will require a waiver explicitly approved by Sigmoid General Manager.

# 5. CONTACT

For security and compliance questions regarding this policy or if you find any violation of the policy, please contact IT Department.

| | |
|---|---|
| **Email** | Infosec@sigmoidanalytics.com, anil.sharma@sigmoidanalytics.com, knaveen@sigmoidanalytics.com |
| **Contact Number** | +91 7972176821 |

# 6. DISTRIBUTION LIST

| Sl. No | Role / Designation | Department |
|---|---|---|
| 1 | All Staff | All Department |
| | | |