Policy on Record Maintenance and Retention Practices

Purpose

This policy outlines the standards and procedures that InGovern Proxy Advisory Services follows to ensure proper maintenance, retention, and disposal of records related to its proxy advisory and research analyst activities. The objective is to comply with applicable laws and regulations, maintain data integrity, support transparency, and safeguard client interests.

Scope

This policy applies to all employees, consultants, and officers of InGovern Proxy Advisory Services involved in the creation, receipt, handling, storage, and disposal of any records (physical or electronic) generated in the course of business activities including research reports, voting recommendations, client communications, and regulatory filings.

Regulatory Framework

InGovern maintains its recordkeeping in accordance with:

- Securities and Exchange Board of India (SEBI) regulations applicable to proxy advisory firms and research analysts
- The Companies Act, 2013, including Rules related to disclosures and maintenance of records
- Applicable guidelines on data security, confidentiality, and audit trails

Record Categories

Records maintained by InGovern include but are not limited to:

- Research reports and proxy voting recommendations
- Client instructions and engagement communications
- Internal review and oversight documents
- Compliance, audit, and monitoring reports
- Correspondence with regulators, companies, and investors
- Confidentiality agreements and conflict disclosures

Retention Periods

Records shall be retained for a minimum period as mandated by SEBI and other statutory authorities, typically:

- Research and voting advisory reports: 5 years from date of issuance
- Client communication and contractual documents: 5 years after termination of contract
- Regulatory filings and compliance documentation: 8 years or as required
- Audit trails and internal governance records: minimum 5 years

Record Storage and Security

- Physical records shall be stored securely in locked facilities with restricted access
- Electronic records shall be stored on secure servers with encrypted backups and access controls
- Periodic audits shall be conducted to verify record integrity, security, and compliance with retention schedules

Record Disposal

- Records exceeding the retention period shall be disposed of securely by shredding (physical) or permanent deletion (electronic)
- Disposal shall be documented to maintain an audit trail
- Records critical to ongoing investigations or legal proceedings shall be retained beyond standard periods until clearance

Responsibility and Compliance

- The Compliance Officer is responsible for implementation, monitoring, and periodic review of this policy
- All employees must adhere strictly to these practices and report any deviations or risks to compliance promptly
- Non-compliance may result in disciplinary action including termination of employment

Policy Review

- This policy shall be reviewed annually or upon changes in applicable regulations to ensure relevancy, effectiveness, and regulatory compliance.

Last updated on 8th October 2025