Edme Insurance
Brokers Ltd.

edme
Clarity in Complexity

EDME Insurance Brokers Limited
Anti-Fraud Policy and Framework

POLICY DETAILS

Policy Title	*Anti-Fraud Policy and Framework*
Policy Owner	*Compliance, Risk Management & Internal Audit*
Policy Author	*Compliance, Risk Management & Internal Audit*
Document Reference Code	*EIBL/AFFPOL/001/2020-21*
Prepared By	*Apurv Mehta*
Reviewed By	*Anurag Dharnidharka*
Approved By	*Board of Directors*
Approval Date	*November 18, 2025*
Effective Date	*November 18, 2025*
Version Number	*2.0*

VERSION CONTROL

Date	Policy Effective	Prepared / Modified by	Reviewed By	Approved by	Version #	Nature of Change
May 08, 2020	May 08, 2020	Apurv Mehta	Punit Pancholi	Board of Directors	1.0	New Policy
November 18, 2025	November 18, 2025	Apurv Mehta	Anurag Dharnidharka	Board of Directors	2.0	Update and aligned to the requirement of Insurance Fraud Monitoring Framework Guidelines issued by IRDAI

Table of Content

1. OBJECTIVE

The objective of this policy is to establish a comprehensive framework in order to deter, prevent, detect, report and remedy fraud risks effectively across all operations and activities of EIBL. It also aims to create awareness amongst the employees about fraud and fraud prevention to facilitate the process owners in developing fraud prevention and detection controls. Further, it aims to enhance the sector's resilience against fraud, foster a culture of integrity, protect policyholders' interests, safeguard financial stability and maintain public trust. It also ensures the compliance of with all the applicable IRDAI guidelines and regulatory requirements related to Fraud Monitoring Framework.

2. SCOPE

This Anti-Fraud policy covers of EIBL at all levels, including Board members and senior management, processes, functions and any entity having any contractual relations with the EIBL.

Also, the following broad categories of fraud are in scope:

- **Internal Fraud -** Fraud committed by internal staff including employees or management
- **Policy holder Fraud / Claims Fraud -** Fraud against EIBL in the purchase and/or execution of an insurance product, including fraud at the time of making a claim.
- **External Fraud -** Fraud committed by staff regardless of their legal relation to EIBL, including temporary workers, third party contractors, interns, consultants or vendors etc.
- **Cyber or New Age Fraud -** Any insurance fraud carried out using digital or new age technologies but not limited to phishing, hacking, online impersonation, malware attacks, data breaches, and unauthorized system access.

3. DEFINITION

- **FRAUD**

  In general, fraud is defined as the deliberate abuse of procedures, systems, assets, products or services by those who intend to deceitfully or unlawfully benefit themselves or others. Fraud is defined as an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. This may be achieved by means of but not limited to :

  - Misappropriating assets/funds
  - Deliberately misrepresenting/concealing/suppressing or not disclosing one or more material facts relevant to any decision
  - Abusing responsibility, position of trust or a fiduciary relationship.

- **RED FLAG INDICATOR**

  A possible warning sign that points to a potential fraud which may require further investigation or analysis of a fact, event, statement, or claim, either alone or with other indicators.

- **ANTI-FRAUD OFFICER**

  Anti-Fraud Officer is a person designated to carry out all the Anti-Fraud activities within the organization. At EIBL, Vice President - Internal Audit, Risk Management & Business Excellence will be designated as Anti-Fraud Officer.

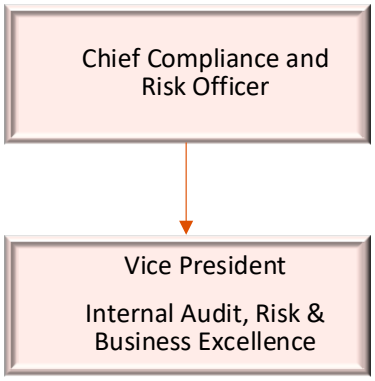
4. FRAUD MONITORING FRAMEWORK

- **FRAUD MONITORING UNIT (FMU)**

Fraud Management Unit is headed by Chief Compliance & Risk Officer who undertakes fraud prevention, detection, investigation and response initiatives. FMU shall also ensure the effective implementation of the Anti-Fraud policy at EIBL and shall also be responsible for the following:

- Creating awareness among the employees /clients to counter frauds
- Laying down procedures for internal reporting from/to various departments.
- Furnish periodic reports to the Board Committee for its review.

All employees of the organization owe responsibility towards the organization to safeguard its assets, report and prevent misuse of assets or breach of procedures. The current structure of the Fraud Monitoring Unit at EIBL is as under:



All Anti-Fraud initiatives span across all units including branches will be managed by Anti-Fraud Officer.

5. ROLES AND RESPONSIBILITIES OF FRAUD MONITORING UNIT (FMU)

The FMU shall be responsible for implementation of the Anti-Fraud Policy within the Company. The Anti-Fraud Officer supports management with regards to all Fraud Control activities in the

company.

The tasks and responsibilities of the Anti-Fraud Officer include:

- Coordinating the implementation of the Anti-Fraud Policy
- Facilitating fraud risk assessments in key areas of the business as per the management requirements
- Monitoring fraud trends and developing fraud alerts
- Creating fraud awareness among employees of various functions through ongoing staff awareness programs and training
- Advising on fraud management and developing fraud prevention, detection & mitigation strategies
- Carrying out control testing and suggest corrective / additional controls if necessary
- Pro-actively engage into an activity to identify potential frauds, red flags and process gaps through process audits or risk framework reviews
- Proactively identify fraud prone vulnerabilities in digital platforms including website, intranet-based portals etc through periodical reviews including review of information security controls
- Reporting fraud to the Board and Senior Management.

6. ROLES AND RESPONSIBILITIES OF BOARD AND SENIOR MANAGEMENT

Management has the primary responsibility for the prevention, detection and investigation of fraud. Management of EIBL must lead by example and shall instill a corporate culture in which unethical and fraudulent behavior is unacceptable. They must take appropriate measures to recover any losses incurred and in principle bring the suspect to justice.

EIBL Board and Senior Management shall be responsible for establishing appropriate and adequate fraud risk management framework and shall:

- Take into account for types of frauds mentioned under clause 4 and relevant red flag indicators, as applicable
- Shall inform the concerned insurer, whenever there is a suspicion of Fraud which may also impact the Insurer, and provide all relevant details.

FRAUD PREVENTION AND DETERRENCE

Fraud prevention activities are the first line of defense against fraud in the organization and include policies, procedure, training and communication. It encompasses any activity which discourages individuals from committing fraud, an example being introduction of fraud related internal controls.

- **TRAINING AND AWARENESS**

  Training, education, and awareness are vital for strengthening fraud prevention efforts. In this regard, EIBL shall conduct:

  - Regular fraud awareness programs educate policyholders and the general public about

the risk of fraud and how to prevent and protect against it.

- Periodic training programs, as appropriate to the functions being carried out for the employees and the senior management including the board members

- **DUE DILIGENCE**

Screening of employees shall be performed before their appointment. Adequate HR policies shall be put in place to conduct background checks and any such screening activity.

- **ADMINISTRATIVE AND INTERNAL CONTROLS**

Internal controls are processes (including elements such as policies, procedures and systems) that are established, operated and monitored by officers responsible for governance and management, to provide reasonable assurance regarding the achievement of the organization's objectives. Internal controls can be both preventive and detective in nature.

A combination of preventive and detective controls enhances the effectiveness of a fraud risk management program by demonstrating that preventive controls are working as intended and identifying fraud if it does occur.

Responsibility of Managers:

All managers must create an environment in which staff members believe that dishonest acts will be detected and investigated. Therefore, EIBL management has a responsibility to ensure:

- Staff members understand that controls are designed and intended to prevent or detect fraudulent behavior;
- Clearly communicate, through policies and statements, that any unethical behavior will not be tolerated
- Take strict action, including disciplinary measures, where there is a misconduct observed or need for corrective measures
- Staff members report suspected fraudulent and corrupt behavior directly to the appropriate manager without fear of disclosure or retribution

The Anti-Fraud officer at EIBL shall ensure that effective preventive and detective controls are in place and are implemented efficiently by conducting risk assessments.

- **PHYSICAL AND USER ACCESS CONTROLS**

Physical security and user access controls are essential in reducing the probability of internal and external fraud by restricting access to computer systems, areas containing sensitive information and areas containing high value assets only to those individuals for whom such information is necessary for carrying out their job responsibilities. Adequate audit trails of access should be maintained.

EIBL have physical security and user access control policy in place which shall ensure the effective implementation of physical and user access controls.

7. FRAUD REPORTING AND RESPONSE

Potential fraud may come to the organization's attention in many ways, including information from employees, customers, vendors such as consultants, outsourced service providers, suppliers, internal audits, process control identification, external audits, or by accident.

EIBL shall have a strong framework in place to report any possible fraudulent activity or significant breaches of controls and deal with it in a timely manner.

- **FRAUD REPORTING**

  All non-whistleblower complaints can be reported to FMU. An endeavor must be made to protect the confidentiality of disclosures made to the whistle blower committee in accordance with the terms of the EIBL Whistleblower's Policy. For further information, please refer to the *Whistleblower's Policy.*

  Every complaint forwarded shall be assessed initially to determine whether there is a case to answer. Anonymous complaints shall not be encouraged as they may be difficult to pursue if further information is required. However, well-substantiated anonymous complaints shall receive appropriate consideration. Frivolous reporting of fraud shall be discouraged as this can cause great personal distress, damage a person's reputation and waste organizational resources. If the complaint is found to be lodged with malafide intentions, appropriate action shall be taken against the person making such frivolous complaint.

  Complaints about suspected fraudulent behavior should, where possible, be written, dated and signed by the complainant. To the extent that information is known or is available, the Complainant shall identify or provide evidence of the following:

  - Details relating to the nature of suspected offence/potential fraud;
  - Details of any staff involved (name and location);
  - Details of any outside parties involved (name, description and address);
  - The time period over which the alleged activity has occurred, if available;
  - An estimate of the monetary value, if appropriate, associated with the alleged incident;
  - Documentary evidence in support of the alleged fraud, where available
  - Contact details of the person reporting the fraud (as further information or assistance maybe required from them to ensure that enquiries and investigations are carried out promptly and efficiently).

  The Anti-Fraud Officer and/or the whistle blower Committee shall be responsible for the receipt of information on suspected instances of fraud.

- **FRAUD INVESTIGATION**

  EIBL shall have a system for prompt, confidential review, investigation and resolution of allegations involving potential fraud. Investigations shall be carried out by the Fraud

Investigation officer. In principle, EIBL shall report fraud to the relevant law enforcement agency in order to initiate proceedings as and when the need arises or as prescribed by the Authority. EIBL shall also lay down procedures to co-ordinate with Law enforcement agencies for reporting frauds on timely and expeditious basis and follow-up processes thereon.

The investigation and response system should be standardized and include processes for:

- Categorizing issues/frauds
- Confirming the validity of the allegation
- Conducting the investigation and fact-finding
- Referral to external parties and use of specialists
- Escalation processes
- Resolving or closing the investigation & recommending corrective actions within the stipulated TAT
- Approval of the corrective/punitive action (if any) by appropriate zonal/ national/ whistleblower committees
- Information management and maintenance of confidentiality;
- Determining how the investigation will be documented;
- Managing and retaining documents and information.

Care needs to be taken in the investigation of suspected fraudulent behavior to avoid unfounded and incorrect accusations, prematurely alerting individuals against whom allegations have been made and making statements that could expose the department to legal liability for damages arising from a wrongful accusation. Individuals undertaking these inquiries/investigations shall have the authority and skills to evaluate the allegation and determine the appropriate course of action and shall act fairly and in good faith without bias, malice, ill will or with improper motives.

Important factors to be considered during designing processes for investigations are:

- **Time-sensitivity** — Investigations need to be conducted in a timely manner due to legal & statutory requirements, to mitigate losses both financial and reputational.
- **Notification** — Certain allegations may require notification to regulators, law enforcement agencies.
- **Confidentiality** — Information gathered needs to be kept confidential and distribution limited to those with an established need.
- **Compliance** — Investigations should comply with applicable laws and rules regarding gathering information and interviewing witnesses.
- **Securing evidence** — Evidence should be protected so that it is not destroyed and so that it is admissible in legal proceedings.
- **Objectivity** — The investigation team should be removed sufficiently from the issues and individuals under investigation to conduct an objective assessment.
- **Goals** — Specific issues or concerns should appropriately influence the focus, scope, and timing of the investigation.

The detailed report prepared by the fraud investigation officer at the end of the investigation

shall capture all the details specified by the complainant (as detailed in the section on fraud reporting) as well as findings against the same and shall recommend the future course of action, both corrective as well as punitive. The Fraud Investigation Unit in Compliance Function shall also be responsible for maintaining an appropriate recording and tracking system to ensure that all instances of suspected fraud are satisfactorily resolved.

8. RECORD KEEPING

The documentation for all the fraud investigation cases shall be maintained for audit trail purpose for the period prescribed by the IRDAI. This should at minimum contain:

- Original informant documentation
- Respondent statements
- Investigation findings & recommended actions
- Copies of documents which may be used as evidence to support the allegation
- Copy of complaint in case complaint is submitted to the local authority or at local police station

9. UPDATING THE POLICY

- The policy review shall be carried out once a year. Board should be notified of the review carried out and needs approval in case of any material changes in the policy. Further, any regulatory changes shall be carried out within 30 days of its issuance.