Edelweiss Life Insurance Company Limited
(formerly known as Edelweiss Tokio Life Insurance Company Limited)

Anti-Fraud Policy

Document Control

Document Name	Edelweiss Life – Anti Fraud Policy
Security Classification	Internal
Location	Mumbai
Owner	CRO

Authorization	
Created / Updated By	**Approved by**
CRO	BOARD

Version	**Board Approved / Review Date DD MM YYYY**
Version 1	14/05/2013
Version 2	15/05/2014
Version 3	15/10/2015
Version 4	11/5/2017
Version 5	19/05/2021
Version 6	15/05/2023
Version 7	25/07/2024
Version 8	29/04/2025
Version 9 (Effective from 1st April'26)	28/01/2026

TABLE OF CONTENTS

1. Background and Purpose

This Anti-Fraud Policy ('the Policy') has been laid down in accordance with the Insurance Regulatory and Development Authority of India (Insurance Fraud Monitoring Framework) Guidelines, 2025. The purpose of the Policy is to establish the measures and controls which will assist in prevention, detection and management of fraud against Edelweiss Life Insurance Company Limited (formerly known as Edelweiss Tokio Life Insurance Company Limited ('the Company'). The Policy intends to lay down the guidance on the development of controls and measures to address and manage risks emanating from fraud and foster a culture of integrity, protect policyholders' interests, safeguard financial stability and maintain public trust. The Policy also defines the guidelines for conduct of investigation and review mechanism to assess the impact of such measures to suggest further corrective steps.

It is the responsibility of all employees of the Company to take all necessary actions to prevent, detect and declare frauds, whenever it comes to their notice. The company upholds a stringent stance against fraud and is fully committed to minimize its occurrence to the greatest extent possible.

2. Definition

- '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, for example, be achieved by means of:
  a. misappropriating assets;
  b. deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to the financial decision, transaction or perception of the insurer's status;

- abusing responsibility, a position of trust or a fiduciary relationship. Red Flag Indicator or RFI means a possible warning sign, that points to a potential fraud and may require further investigation or analysis of a fact, event, statement, or claim, either alone or with other indicators.

- 'Cyber fraud' refers to fraudulent activities executed through digital or emerging technologies by individuals with malicious intent. It involves exploiting vulnerabilities in systems, processes, or people, leading to insurance fraud and posing significant risks to data security, system integrity, financial transactions, and customer trust.

3. Scope

The Policy covers both internal as well as external frauds. It applies to any fraud or suspected fraud involving employees as well as policyholders, insurance agents, insurance intermediaries, consultants, vendors, service providers, contractors and any other outside agencies or third parties having a business relationship with the Company across all distribution channels including e-commerce.

4. Classification of Insurance Frauds

Insurance Frauds may broadly be classified as under:

a. Internal Fraud – It is a fraud in which, any employee or officer of the company, may or may not, with the aid of his/her associate (family, friend, close relations, etc.) act fraudulently causing direct/indirect loss to the Company, its employees, its policyholders or any counterparty. It can include frauds outside the Company but impacting the Company's performance.

b. Policyholder Fraud and/or Claims Fraud - Fraud against the Company in the purchase and/or execution of an insurance product, including fraud at the time of making a claim.

c. Distribution Channel Fraud (Insurance Agent, Distribution Partner, Insurance Intermediary) - Fraud perpetuated by an insurance agent, Insurance Intermediary (Corporate Agent, Insurance Broker, Web Aggregator, Insurance Marketing Firm) against the Company and/or policyholders.

d. External Frauds – Fraud, including cyber fraud, against the Company conspired by any external consultants, vendors, contractors, service providers or any other external agencies or third parties, regardless of whether they have a business relationship with the Company.

e. Affinity Fraud or Complex Fraud - Fraud involving collusion among one or more fraud perpetrators in the above categories.

Additionally, there are different type of malpractices like Mis-selling, Third party payment, Renewal deposit lapping, Ghost Employees (refer Annexure I for details) etc.

5. Fraud Risk Governance

The Risk Management Committee ('RMC') of the Board and the Fraud Management Committee (FMC) hold the primary responsibility of effective implementation and

oversight of the fraud risk management framework. The Fraud Monitoring Unit (FMU) of Risk Management Department is responsible to translate the management's Fraud Management vision to set up robust Company-wide fraud management practices across all levels.

Fraud Monitoring Committee (FMC) which shall be responsible for operationalizing the Fraud risk management framework within the insurer and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

Function of Fraud Monitoring Committee (FMC) shall be responsible for:

a) recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
b) oversee prompt responses to instances or suspicions of fraud
c) maintain all relevant details pertaining to each instance of fraud
d) facilitate collaboration with industry peers / bodies, law enforcement agencies and regulatory bodies to pursue cases of fraud and share information / intelligence on known fraud schemes and perpetrators.
e) conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc & submit the report before Board of Directors through RMC.
f) identify areas for improvement and adaptation of the Fraud Risk Management Framework.
g) submit quarterly reports to the RMC on its activities, findings, and recommendations including the financial impact of fraud on the insurer
h) report to the Audit Committee, in addition to the RMC, in case of all internal frauds.

The Fraud Monitoring Unit (FMU) of Risk Management Department, independent from internal audit, to support FMC in discharging its functions and effective implementation of measures suggested by FMC. The FMU shall implement the Fraud Risk Management Framework and shall be responsible for the following:

a. investigating the reported frauds as per the laid down investigation procedure including evidence gathering, and collaboration with relevant departments for investigation and submission of investigation report. Conflicts of interest shall be identified and avoided throughout the investigation process
b. reviewing fraud prevention and mitigation measures to ensure its efficient functioning;
c. periodic identification, measurement, control and monitoring of fraud risk and reporting of their findings to the Fraud Monitoring Committee (FMC) for taking necessary actions to correct system and processes gaps accordingly.

d. quarterly reporting of identified fraud cases to Fraud Monitoring Committee (FMC)
e. maintaining transactional-wise details of fraud including action taken
f. collaborating with industry peers / bodies, law enforcement agencies and regulatory bodies to pursue cases of fraud and share information / intelligence on known fraud schemes and perpetrators.
g. conducting fraud-sensitive audits for compliance with the Fraud Risk Monitoring Framework
h. tracking business trends from distribution channels, continuously monitoring vendor activities for compliance with fraud prevention measures and contractual obligations,
i. analysing customer grievances and complaints to detect and prevent fraud.
j. review process to identify the missed insurance fraud detection opportunity
k. Conduct fraud-sensitive audits for compliance with the Fraud Risk Monitoring Framework
l. maintain an Incident Database of persons convicted of or attempting fraud

The function head of FMU shall ensure reporting incidents of frauds and submission of regulatory reports.

6. Fraud Risk Management framework

The Fraud Risk Management framework aims to ensure that the Company is adequately equipped to protect its brand, reputation and its assets from loss or damage resulting from suspected or confirmed incidents of internal or external frauds/misconducts.

a. Fraud Risk Identification

Risk, HR, Operations, Finance & Accounts, Compliance and Assurance/IA Departments shall have the joint responsibility for detecting and monitoring frauds. The concerned department heads shall oversee the end-to-end process from detection to corrective actions against identified frauds.

All employees of the Company have the responsibility of detecting potential fraud and should be alert for any indication of irregularities. Every employee shall report any confirmed, attempted or suspected fraud at the earliest, via designated email ID at fraud.prevention@edelweisslife.in.

Any person with knowledge of confirmed, attempted or suspected fraud who is personally being placed in a position by another person to participate in a fraudulent activity will have to report the case at the aforesaid designated mechanism. Fraud Monitoring Unit shall, on receipt of such communication, analyse and decide on further course of actions. Fraud Monitoring Unit can also suo moto take cognizance of complaints received from other sources like whistle blowing, customer complaints, etc.

Fraud Monitoring Unit (FMU) team shall conduct review of policies to identify any suspected fraud cases basis red flag indicators (RFIs), statistical analytics & earlier experience of the company.

Any withholding of known information about any committed, attempted or suspected fraud by any person could be taken very seriously and results in disciplinary actions.

b. Investigation

The Fraud Monitoring Unit (FMU) is entrusted with the full authority for the investigation of all suspected/actual fraudulent acts as defined in this Policy. The examination of a suspected fraud (or a transaction) or a customer dispute/alert shall be undertaken by the Fraud Monitoring Unit (FMU) or the appointed investigation agencies (as appropriate). Fraud Monitoring Unit shall investigate the frauds (including internal frauds and employee mis conduct) within the Company in an unbiased manner.

The first step in an investigation process is gathering and validation of case facts. In order to investigate into suspected cases, the Fraud Monitoring Unit (FMU) would adopt to various techniques during the course of investigation. The investigation team may conduct oral interviews of customers, employees, advisor to understand the background and details of the case. In case an interview of the person accused of fraud is required to be undertaken, the investigation team will follow a prescribed procedure and record statements appropriately. The investigation activities will be carried out discreetly and within a turnaround time (TAT) as may be specified.

The investigation report will conclude whether a suspected case is a fraud and any form of involvement of employee in the act of fraud. In special circumstances, the investigation into suspected fraud cases may be assigned to external specialised agencies considering various circumstances such as non-availability of specific expertise in the Company or lack of physical presence at a particular geographic location.

The complainant and everyone involved in the investigation process shall maintain complete confidentiality/ secrecy of the matter and shall not discuss the matters under this Policy in any informal/social gatherings/ meetings.

Fraud Monitoring Unit (FMU) team shall investigate the spurious call complaint cases & take appropriate actions.

c. Taking Corrective Actions

The Fraud Monitoring Unit (FMU), on closure of the investigation, shall share the decision to the respective department. It shall also ensure in collaboration with legal & HR that appropriate action is taken against the perpetrators.

d. Co-ordination with Law Enforcement Agencies

Streamlined coordination with law enforcement agencies ensures that fraud incidents are brought to conclusion in a timely and an effective manner.

(i) Based on the investigation conducted and recommendation made, in collaboration with Legal team, Fraud Monitoring Unit (FMU) team to ensure coordination with the law enforcement agencies to get the complaint registered on a need basis.

(ii) Fraud Monitoring Unit (FMU) team of the company shall be responsible to attend to the law enforcement agencies for the investigation purpose. As the case may be Fraud Monitoring Unit (FMU) team shall extend the required assistance to the law enforcement agencies.

e. Preventive Mechanism

Preventive measures are crucial for managing the risk of fraud effectively. The company must establish suitable procedures and controls to proactively prevent fraud occurrences. Determining the extent of necessary controls should be guided by a comprehensive risk analysis, with a focus on identifying potential indicators of fraud. Each department should incorporate appropriate checks and balances into their internal Standard Operating Process Manual to thwart fraudulent activities. Furthermore, the company should conduct due diligence on all personnel (including management and staff), insurance intermediaries, third-party administrators (TPAs), and external vendors before engaging with them or entering into agreements.

Further, the company has a Whistle blower policy in place to report any incident/event as detailed in that policy.

7. Database Building and Information Exchange

The Company shall closely work with various industry players/ Councils/Forums/Regulator etc. to enhance mutual cooperation and exchange best practices.

IIB is a centralised fraud database to which the companies shall share information. Co-operation amongst life insurance players is a must for successful detection of fraud and gaining from other's experience. IIB shall be used as centralised database & information exchange for:

a. Sharing fraudulent policy details;
b. Sharing of information regarding distribution channels, hospitals, third party vendors and fraud perpetrators those who committing frauds with IIB

8. Cyber Fraud

Cyber fraud threatens identity security, financial integrity, and reputation by exploiting vulnerabilities in systems. The company shall have a robust cybersecurity framework to safeguard customer data and business integrity & to combat evolving cyber fraud threats. The company shall ensure continuous monitoring and strengthening of system and processes for fraud risk management, including identity verification, incident tracking, distribution channel risk assessment, access controls etc.

9. Risk Monitoring and reporting of Frauds

The results of risk measurement and control for fraud risk should be published and reviewed by the Committee which in turn must present a summary to the Board on a regular basis. The Company shall prepare an annual report on the fraudulent cases along with the actions initiated by the Company, in the format as prescribed by IRDAI (FMR-1). The Report shall be submitted to IRDAI within 30 days from the close of the financial year. In the event of fraud committed by distribution channels registered by IRDAI, the insurer shall promptly escalate and report the matter to IRDAI without delay.

10. Training and internal Communication

A risk awareness culture should be developed by improving understanding, communication and education. Customer awareness is one of the pillars of fraud prevention.

The Company shall ensure periodic training programs to the functions being carried out for the employees and the senior management including the board members, as appropriate.

The Company shall ensure that the communication to the customer, general public, employees, insurance agents, distribution partners, insurance intermediaries and other relevant stakeholders is simple and aimed at making them aware of fraud risks including cyber frauds.

11. Amendments and Review

This Policy can be amended any time during the year either on the basis of the recommendations of the Board, the Risk Management Committee or as and when the Company considers it is appropriate based on feedback, changing business environment etc. The amendments approved by the Risk Management Committee shall be put up to the Board, at its next meeting, for ratification. The policy shall be reviewed on an annual basis.

This policy shall be effective from 1st April 2026.

Annexure – I

Illustrative List of Insurance Frauds

Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

1. Internal Fraud:

a) misappropriating funds
b) fraudulent financial reporting
c) stealing cheques
d) inflating expenses claims/over billing
e) paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
f) permitting special prices or privileges to customers, or granting business to favoured suppliers, for kickbacks/favours
g) forging signatures
h) falsifying documents
i) Impersonation, death prior proposal at sourcing of policy

2. Policyholder Fraud and Claims Fraud:

a) Staging the occurrence of incidents
b) Reporting and claiming of fictitious damage/loss
c) Medical claims fraud
d) Fraudulent Death Claims

3. Distribution Channel fraud:

a) Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the insurer
b) Inflates the premium, passing on the correct amount to the insurer and keeping the difference
c) Commission fraud - insuring non-existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

4. External Fraud

a) Financial misappropriation done with the company by third parties not having any business relationship with the company
b) Cyber frauds
c) Frauds by external consultant, vendors, contractors, service providers etc.
d) Gaining unauthorized access to company assets etc.

5. Affinity fraud or complex fraud

a) Financial misappropriation done by distribution channel in connivance with the employee.
b) Frauds by external vendor in connivance with the employee.

Various definitions of malpractices are given below:

Mis-selling – Mis-selling refers to the practice of a seller, selling a product or service in a misleading or inappropriate way. This can involve not providing enough information, giving incorrect advice, or persuading customers to buy products that are not suitable for their needs. Mis-selling can lead to financial losses and other negative consequences for the consumer.

Third party payment – Where the premium payment for the policy has been done by seller or any other person, having no insurable interest.

Renewal Deposit Lapping – Where the seller has collected the renewal premium from a customer but has not deposited it with the company. The renewal payment of the said customer is managed through the renewal premium collected from another customer. The process continues with new deposits being used to cover the renewals of earlier deposits, thereby concealing the initial misappropriation.

Ghost Employee - A ghost employee is a non-existent employee who is listed on an organization's payroll. This fraudulent practice involves creating fictitious employees or retaining names of former employees on payroll records, allowing someone (usually a person within the company) to collect their salaries.

==========