HDFC ERGO GENERAL INSURANCE COMPANY LIMITED

Anti-Fraud Policy

Created by		Fraud Control & Monitoring Unit (FMU) (Fraud Control Unit (FCU) and Risk and Loss Mitigation (RLM) units together)									
Concurred by		Legal & Compliance									
Review Period		Annual									
Version	Version 1.0	Version 1.1	Version 1.2	Version 1.3	Version 1.4	Version 1.5	Version 1.6	Version 1.7	Version 1.8	Version 1.9	Version 2.0
Approved by Board of Directors on	August 18, 2017	January 24, 2018	October 22, 2018	October 23, 2019	January 22, 2020	January 21, 2021	January 25, 2022	October 20, 2022	October 12, 2023	October 11, 2024	January 13, 2026
Effective From	August 18, 2017	January 24, 2018	October 22, 2018	October 23, 2019	January 22, 2020	January 21, 2021	January 25, 2022	October 20, 2022	October 12, 2023	October 11, 2024	April 1, 2026

Anti Fraud Policy

1. Introduction:

Fraud poses a serious risk to all segments of the financial sector. The insurance business by its very nature is susceptible to fraud. While it impacts the Company's reputation, goodwill and finances, it can significantly erode the confidence of the policyholders and shareholders. Customers too are directly impacted as the increase in premium to offset losses due to frauds is to be borne by them. The overall impact of fraud is therefore a significant cost to the industry as well as to the consumers.

In order to provide regulatory supervision and guidance on the adequacy of measures taken by insurers to address and manage risks emanating from fraud, the IRDAI vide IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025 [Ref No: IRDAI/IID/GDL/MISC/112/10/2025] dated 9th October 2025 ("**Circular**") laid down the Guidelines requiring insurance companies to target zero tolerance for fraud and put in place appropriate Fraud Risk Management Framework to deter, report and remedy Insurance Frauds. The Circular mandates all insurance companies to put in place, as part of their corporate governance structure, a Fraud Risk Management Framework and a Fraud Monitoring Committee which will identify, mitigate and monitor the various categories of fraud.

Accordingly, this Anti-Fraud Policy ("**Policy**") lays down the framework adopted by the Company to implement mitigation measures and pro-active fraud detection framework.

2. Objectives of the Policy:

The key objectives of the Policy are as follows:

- To establish a comprehensive Fraud Risk Management Framework to deter, prevent, detect, report and remedy the incidences of frauds and other irregularities.
- To lay down fraud detection parameters for the insurance e-commerce activities. Cases are detected proactively through analytics, mystery shopping and investigation of the cases received from various known and unknown sources / persons.
- To establish an independent unit - Fraud Monitoring & Control Unit (FMU), which would be collectively both, the Fraud Control Unit (FCU) and Risk and Loss Mitigation Unit (RLMU), to identify, detect and investigate suspected fraud cases. Investigation of such cases is to be carried out by FMU.
- To constitute a Fraud Monitoring Committee (FMC) to take necessary remedial action on all fraud cases reported or violation of Code of Conduct: Decision making process is done through duly constituted FMC.

3. Definition, meaning and understanding of fraud

Fraud is a term which generally refers to any act committed intentionally to secure an unfair or unlawful gain. This wrongful gain through deceit can be made either singly or jointly with others.

Frauds can be committed by clients, intermediaries, impostors, petitioners, third party administrators, vendors and even by the internal staff of the companies. Apart from that professional syndicates operate all over the country.

The frauds that could be perpetrated against the Company inter alia includes embezzlement, bribery, vendor related third party frauds, money laundering, etc. The risk of employees tinkering with the confidential information and colluding with fraudsters is also prevalent.

Reasons for the frauds are mainly:

- Opportunity of getting very high rewards with minimal possibility of detection
- Penal provisions extremely soft having very low prosecution
- Victimless and easy to commit
- Insurance frauds are hardly considered as social stigma. In fact, most of these are taken as accepted practice by the society
- Insurance frauds are very low on priority for law enforcement agencies
- Opportunity for the business houses in distress to compensate for the losses
- Weak internal systems & processes
- Lack of effective vigilance and investigation mechanism

Insurance Fraud shall mean an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties, including but not limited to:

- Misappropriating Fraud
- Deliberately misrepresenting/concealing/ not disclosing one or more material facts relevant to any decision/transaction, financial or otherwise.
- Abusing responsibility, position of trust or a fiduciary relationship.

Red Flag Indicator/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.

Distribution Channel include insurance agents, intermediaries or insurance intermediaries, and any persons or entities authorized by IRDAI to involve in sales and service of insurance policies.

Cyber or New Age Fraud means any Insurance Fraud carried out using digital or new age technologies.

Law Enforcement Agencies (LEA) shall mean any governmental authority or agency legally empowered under applicable laws, including the Prevention of Money Laundering Act, 2002 (PMLA), to investigate, prevent, or prosecute offences. This includes, but is not limited to:

- Enforcement Directorate (ED) and officers appointed under Sections 48 and 49 of PMLA
- Police authorities at State and Central levels
- Customs and Central Excise Departments
- Income Tax Department
- Reserve Bank of India (RBI)
- Securities and Exchange Board of India (SEBI)
- Any other statutory or regulatory body notified under Section 54 of PMLA or other applicable laws

4. Fraud Control and Monitoring Unit (FMU) [Collectively the Fraud Control Unit (FCU) and Risk and Loss Mitigation Unit (RLMU)] and its Functions:

The **Fraud Control and Monitoring Unit (FMU**), which shall operate under the guidance and oversight of a **Fraud Monitoring Committee (FMC),** and in accordance with the **Fraud Risk Management Framework** and would discharge its functions including those listed below, towards ensuring a zero-tolerance approach toward fraud:

- To put in place Fraud Monitoring Framework that appropriately measures to identify and assess fraud risks.
- To identify potential areas of frauds through data analytics and formulate RFIs
- To evaluate and review Red Flag Indicators periodically (at least annually).
- To put in place control measures with regards to frauds.
- They shall monitor and maintain an incident database of persons convicted or attempted fraud conducting fraud sensitive audits for compliance with Fraud Risk Monitoring Framework. They shall:
  - Track Business trends from distributing channels,
  - Continuously monitor vendor activities for compliance with fraud prevention measures and contractual obligations and
  - Analyse customer grievances and complaints to detect and prevent fraud.

- It shall report the status of significant cases of fraud detected in the Company to the Fraud Management Committee and to the Board of Directors on a quarterly basis through the Risk Management Committee of the Board. FMU shall also maintain records of cases of frauds, as investigated by it, from those having intimated under Whistleblower Policy as well.

- In performing their duties under this Policy, the members of the FMU will have free and unrestricted access to all Company records and premises, whether owned or rented, and the authority to examine, copy and/or remove all or any portion of the contents of files, desks, cabinets and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation, subject to approval of the FMC.

5. Fraud Risk Management Framework entails fraud identification and monitoring through established red flag indicators, timely investigation and mitigating impact of frauds followed by requisite reporting within the general principles, some of which are articulated herein the Policy.

The **Fraud Management Committee** shall guide the **Fraud Monitoring and Control Unit** to adhere to the Fraud Risk Management Framework.

I. <u>Principles to be followed in Fraud Monitoring Framework:</u>

- **Principle of proportionality**: In taking anti fraud measures, the Company must recognise the principle of proportionality i.e. the measures adopted to mitigate frauds must be in proportion to the risks involved.

- **Zero tolerance:** Any activity with the intention of perpetuating fraud against the Company shall not be tolerated. Any individual involved in a fraudulent activity will be subject to sanctions up to and including dismissal from services of the Company. The Company may further take criminal or civil proceedings under applicable laws. In case of agent/intermediary/Vendor/TPA

who fail to adhere to this Policy, the Company may terminate its relationship with them or may further take criminal or civil proceedings under applicable laws.

- **Full investigation:** Suspected fraudulent activity must be investigated immediately by FMU. FMU may deploy external consultants or seek assistance of government bodies as it deems fit. If the investigation establishes a strong suspicion of violation of the law, the Company reserves the right to take any action including but not limited to civil and criminal prosecution. The details in this regard have been highlighted in the Policy hereunder.

- **Compliance with law and internal policies:** The Company shall ensure that while implementing the anti-fraud measures, the applicable laws and internal policies of the Company must be strictly complied with. This also applies where the help of external consultants is taken to investigate a case of fraud.

- **Documentation:** Anti-fraud management activities and measures must be clearly documented and records maintained for the period as identified in the Document Retention Policy of the Company. Where a case of fraud is the subject of investigation, care must be taken to ensure that, as far as possible, all evidences are available in a form admissible in court.

- **Regular review and refinement:** The components of anti-fraud management and associated measures, especially the effectiveness of internal controls, must be reviewed on a yearly basis.

II. Classification of Frauds:

Internal Fraud: Fraud involving internal staff, including employees and/or senior management, and entails, **financial Misconduct,** which includes misappropriation or siphoning of funds, fraudulent reporting, financial impropriety, utilisation of company funds for personal purposes, underwriting frauds, frauds by employees and violation of the Company's Code of Conduct.

Distribution Channel Fraud: Fraud involving distribution channels, including premium misappropriation and misrepresentation.

Policyholder Fraud and/or Claims Fraud includes frauds while obtaining coverage or payment during the purchase, servicing or while seeking claim of an insurance policy.

External Fraud: Fraud involving external parties, service providers, vendors, etc.

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

III. Indicative methods of fraud identification:

- Periodic data analytics resulting from the RFIs
- Periodic checks on processes and policies

IV. Red Flags Indicators or RFIs:

RFIs 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. The RFIs alongwith the monitoring controls and primary function related are detailed in the Annexure to this Policy, and the said Annexure shall be treated as an integral part of this Policy.

V. Cyber or New Age Fraud

- To collaborate with the cybersecurity risk management team to establish and implement robust cybersecurity framework, which in turn supports cyber fraud risk management
- Continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control.

VI. Fraud Intimation:

All persons including employees, vendors, TPAs, agents, intermediaries are expected to take all reasonable steps to prevent the occurrence of Frauds including cyber and online frauds and to identify and report instances of known or suspicious Fraud committed against the Company, whether by the employees or by outside parties. All employees should report any Fraud including Cyber / Online Fraud against the Company to his immediate senior or to the FMU at fraudintimations@hdfcergo.com.

6. Fraud Investigation procedures:

FMU shall be responsible for investigating and handling all cases highlighted as Frauds. It shall take prompt and appropriate action with respect to such frauds to remediate the circumstances giving rise to occurrence of such frauds.

- **Investigation & Evidence Gathering:**
  - Conduct detailed investigations into potential fraud incidents while ensuring no conflict of interest. In case of conflict of this Policy with any internal Standard Operating Procedures, it will have an over-riding effect and shall prevail upon. Subsequently the user department should take steps to eliminate such conflict.
  - Further, it shall also analyse the data based on frauds detected during field investigations.
  - FMU shall investigate the cases with 45 days; it shall intimate the FMC in advance should it not be able to investigate any case within the aforesaid timelines
  - FMU shall investigate all such cases and render report to the Fraud Monitoring Committee (FMC) duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any.
  - FMU shall be responsible for implementing the decisions by FMC & the WBCC, wherever applicable and impacted
  - FMU shall track the closure of the decisions through Action Taken Report (ATR).
  - FMU shall collate all cases of frauds reported to it through various channels, entities including the Whistleblower Complaints Committee (WBCC).
  - FMU shall maintain full authority to access company records, premises, and digital data (emails/files) for investigative purposes.

- FMU shall report the status of significant cases of fraud detected in the Company to the Fraud Management Committee and to the Board of Directors on a quarterly basis.

- **Database & Intelligence Management:**
  - Maintain a comprehensive incident database of persons convicted of or attempting fraud.
  - Participate in the **Insurance Information Bureau (IIB)** technology framework to share data on blacklisted distribution channels, hospitals, vendors, and known fraud perpetrators. The same shall in the accordance with the extant applicable data privacy laws.

- **Investigation of Fraudulent Claims** – All suspected fraudulent claims shall be investigated by a dedicated team constituted under the FMU. Status of significant cases of suspected frauds detected shall be informed to the Head of respective Claims Teams (based on LOBs) on a regular basis. Dedicated Outsourced Agencies and in-house personnel would be deployed to carry out verification as well as checking the authenticity of documents provided at the time of claim. All claim frauds shall be investigated with a view to ensure adherence to regulatory TATs for settlement of claims thereafter.

- Complaints/disclosures made against or in relation to employees of the Company shall be dwelt in accordance with the Whistleblower Policy and complaints/disclosures against any person / entity other than employees of the Company shall be dwelt in accordance with the provisions of this Policy

- The Department Heads shall be responsible to take actions as per the decision of the FMC. Further, the Departmental Heads shall be responsible to act on the recommendations of FMU which it may render from time to time to improve any System and Process gaps.

- No employee shall investigate / interview / interrogate such cases of actual / suspected frauds himself except the responsible person within FMU.

- **Confidentiality and Non – Retaliation:** Under the Policy, every reasonable effort shall be made to ensure the confidentiality of the person who has reported the Fraud. The identity of those providing information shall be kept confidential in order to carry out an appropriate, fair and thorough investigation. If a fraud is reported anonymously, the person must provide credible and sufficient information to enable the FCU to investigate. The Company shall ensure that no retaliatory action is taken against any individual for reporting, in good faith, known or suspected Fraud.

7. Fraud Monitoring Committee (FMC):

FMC shall be constituted to review the findings of the investigations done by FMU and to take appropriate actions thereupon. The FMC 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.

I. Composition of FMC: The FMC comprises:

- Executive Director & CFO
- Executive Director
- Director & Chief Business Officer
- President & CHRO

II. Role and functions of FMC:

a. FMC shall recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
b. FMC shall oversee prompt responses to instances or suspicions of fraud
c. FMC shall be presented all relevant details pertaining to each instance of fraud.
d. FMC shall 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. FMC shall 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.
f. FMC shall identify areas for improvement and adaptation of the Fraud Risk Management Framework

Head of the Department of the accused shall be invited at the meetings of the Committee without having any right to vote. In case a lady is summoned by the Committee then a lady employee of SM2 and above grade shall be co-opted as an observer. The Company Secretary and Chief Compliance Officer shall be the permanent invitees at the meetings of the Committee and inter-alia record the proceedings of the meeting and safe custody of said minutes ensuring its confidentiality.

III. Frequency of Meeting

The Committee shall meet atleast on a quarterly basis with a provision for seeking decision through circulation to decide on urgent cases. Such decisions shall be noted at the immediate next meeting of the Committee. The Committee shall be responsible inter-alia for effective implementation and to monitor and decide fraud cases.

IV. Quorum: The quorum for the meetings of the Committee shall be at least three members.

V. Conflict Management:

- In case of Complaints against any members of FMC, the concerned member shall not attend the meetings of FMC wherein the subject matter is being discussed. Further, in case such matter requires investigation by FMU, the concerned member shall restrain from initiating any instruction to the FMU.

- In case of Complaints against the Managing Director and Chief Executive Officer and other Whole-Time Directors, the same shall be reported to the Nomination and Remuneration Committee of Directors.

8. Consequences of failure to comply with the Policy:

The Company expects all its employees to act in full compliance with this Policy in conjunction with the Code of Conduct, Whistleblower Policy and such other policies in a manner consistent with the highest ethical standards. This Policy and its relevant provisions shall be adequately publicised and

made known to all concerned including employees, agents, intermediaries and other channel partners.

Any employee found to have been involved in a fraudulent activity or other misconduct or to have failed to report a known or suspected instance of Fraud will be subject to disciplinary action up to and including termination. Furthermore, such conduct of the employees or other parties if found to be in violation of the law then it may result in civil or criminal action.

Failure to adhere to this Policy may result in appropriate actions pursuant to this Policy

The Policy shall be hosted on the intranet of the Company with the objective of creating awareness amongst the employees and an excerpt of the same shall be put up on the website of the Company for the consumption of intermediaries and policy-holders to counter insurance frauds.

9. Preventive Mechanism:

Due Diligence:

- ***Responsible Department for onboarding***
  - The HR Department shall conduct due diligence of employees at the time of on-boarding.
  - The due diligence of intermediaries, channel partners, vendors, Hospitals, Garages etc. shall be carried out by the respective departments.

- ***Procedure for onboarding***
  - The Company shall have requisite standard operating procedures in place w.r.t. due diligence and empanelment of insurance agents and insurance intermediaries and should strictly abide by the same
  - Prior to empanelment of an insurance agent or entering into an agreement with any insurance intermediary, the Company shall carry out requisite due diligence taking into account factors such as security, business continuity, etc. wherever applicable.

- The FMU may suggest documents/information that may be collected from all/some or identified intermediaries (proposed to be empanelled), based on the judgement of the 'Designated Person' (as authorized pursuant to IRDAI requirements).

- In case of default, appropriate actions shall be undertaken against the insurance agent / insurance intermediaries / TPA as per applicable IRDAI Regulations and terms of the agreement.

- All employees shall be required to confirm their adherence to this Policy and declare any Conflict of Interest, once in a year.

Awareness:

Awareness interventions for both potential clients and existing clients about frauds shall be done. Appropriately and necessary caution in the insurance contracts/relevant documents, duly highlighting the consequences of submitting a false statements and/or incomplete statement to be included, for the benefit of the policyholders, claimants and the beneficiaries.

Periodically awareness campaigns, against frauds, for all employees, shall be ensured.

A brief training on prevention of frauds shall be imparted to all new entrants during the induction training.

10. Applicability of the Policy:

The Policy is to be read in conjunction with the Code of Conduct and Whistleblower Policy and is intended to supplement / compliment all applicable laws, rules and regulations and other corporate policies.

All employees shall confirm to having read and understood this Policy and not violated any of its provision, on an annual basis, in the form as may be advised by the HR Department. All new joiners shall adhere to this requirement also at the time of joining the Company.

11. Review of the Policy

This Policy shall be reviewed by the RMC and the Board as follows:

1.1 At least once in every financial year, or

1.2 As and when the RMC and/or the Board considers it appropriate, or

1.3 As and when the underlying laws governing the Policy undergo any change.

Annexure

Red Flag Indicators:

Classification of Fraud	Red Flag Indicators and Monitoring Controls	Remarks for coverage
Policyholder & Claims Fraud	Close Proximity claims	Motor & Health Claims
	Fake / Manipulated Documentation	Motor & Health Claims
	Misrepresented claim information	Motor & Health Claims
	Reimbursement claim from Network post Cashless Denial	Health Claims
	Multiple diagnosis and treatment for infectious disease form primary / secondary care	Motor & Health Claims
	Claim from Negative list of Hospitals / Customers	Motor & Health Claims
	Multiple sources of Seat of Fire / Origin	Property Claims
	Claim related Bills in serial order	Motor & Health Claims
	AI based multivariate trigger systems for suspected claims	Motor & Health Claims
Affinity fraud / Complex fraud	Premium Siphoning: Identification / tracking of unauthorised links / website on internet having Company's name	All LOBs Sales and UW
Internal fraud	Commission Siphoning: Employee / Relatives details (PAN, Contact details of self / family) matched with Agent's details	All LOBs Sales and UW
	Negative / bypass penny drop cases pertaining to motor & health claims	Claims
	Irregular Patterns of employee Expense reimbursement	All employees
Internal / Distribution / Affinity fraud	Refund Siphoning: Same bank account number/s used for refund of premium for multiple policies	All LOBs

Please note that parameters for the aforesaid triggers are dynamic and would vary depending on the evolving use of any particular method(s) and hence are not prescribed here; the FMU shall highlight the same to the FMC periodically, which shall review the same alongwith the aforesaid RFIs

Product wise segment of frauds & procedures for fraud monitoring:

- **Frauds in Health segment:** At the individual level, mostly there are impersonations, non-disclosure / hiding of material facts with regard to pre-existing diseases/other policies. The claims are based on totally fabricated/manipulated documents. High value Personal accident claims are made by manipulating the forms of death (like conversion of suicide into Road Accident) to bring it within the policy coverage. At the hospital level, they fabricate claims, inflate bills for services not provided, perform unwanted diagnostics/surgeries and convert OPD cases into IPD etc. In many cases the diseases outside the coverage are treated but substituted with those permitted. Cases of fake/non-existent hospitals running the rackets are also quite common.

- **Frauds in Motor segment:** In this segment, frauds can very broadly be classified under three categories i.e. under Third Party, Own Damage and Theft.

In the **Third Party** segment, staging accident/ injury/ arson, antedating of cover note, collusion of internal/ external persons with the claimant to help him get inflated claim, granting cover but not depositing the premium are the most common types of frauds. A large number of fleet owners do not renew the policies of most of their vehicles, however, when accident occurs to any of those vehicles, they substitute it with those having insurance cover. Misrepresentations of facts with respect to permit violation, driving license validity etc are quite common. Staging of altogether fake claims by the fraudsters through implanting of fake petitioners/witnesses in connivance with the unscrupulous police officials, advocates are other areas of concern. Filing of double petitions, lodging claims with many companies, conversion of gratuitous passengers as pedestrians, conversion of other type of accidents to Road Traffic Accident, creation of fake employer-employee relationship for Workmen compensation are some of the other very commonly noticed frauds.

In the **Own Damage** segment, staging of accidents, concealment of previous damages, substitution of ineligible person driving vehicle without a valid license are the major frauds. Misrepresentation of facts with respect to MLC, Post mortem reports, illegal hire & reward activity etc are some of the other areas of frauds found very commonly.

In **Motor Theft,** Vehicles impounded by the law enforcement agencies for illegal acts and those seized by the financers on account of default in payments are very conveniently reported as stolen to the insurance companies. Selling off the vehicle or hiding a vehicle in remote locations and then reporting it as stolen are another set of practices. In many cases, the vehicles are totally dismantled and then parts are sold in pieces leaving no trace of theft whatsoever. Non availability of centralized database with the RTOs makes execution of these acts very easy.

- **Frauds in Property segment:** The property claims are generally large by value and mostly the cause attributed to is accidental fire. More often than not through forensic investigation it is observed that companies in distress resort to arson.

- **Frauds in marine segment:** The transporters segment is highly disorganized where the fly-by night operators are plenty in the market. High value transit items like medicine are subjected to pilferage/ theft with their connivance leading to huge leakages. Recovery process through courts is not only very lengthy and time consuming but also expensive.

- **Examples of some other important types of frauds:**
  - Vendor fraud (e.g. Consideration including the receipt of excessive gifts or accepting or seeking anything of material value from contractors, vendors or persons providing services/materials);
  - Forgery or alteration of documents or accounts belonging to the Company;
  - Concealment or misrepresentation of transactions, assets or liabilities;
  - Expense report fraud (e.g. claims for services or goods not actually provided, seeking fake reimbursements);
  - Loss of intellectual property (e.g. disclosing confidential and proprietary information to outside parties);
  - Conflicts of Interest resulting in actual or exposure to financial loss;
  - Embezzlement (e.g. misappropriation of money, securities, supplies, property or other assets);
  - Cheque fraud (forgery or alteration of cheques, bank drafts or any other financial instrument);
  - Payroll fraud;
  - Bribery & corruption (misusing the vested authority to seek personal gains);

- Fraudulent financial reporting (e.g. forging or alteration of accounting documents or records; intentional concealment or mis-statement of transactions resulting in falsification of records or misleading statements;
- Intentional failure to record or disclose significant information accurately or completely
- Improper pricing activity;
- Unauthorized or illegal use of confidential information (e.g. profiteering as a result of insider knowledge of company activities);
- Electronic Fraud and/or illegal hacking, unauthorized or illegal manipulation of information technology networks or operating systems;
- Tax evasion;
- Destruction, removal or inappropriate use of records, furniture, fixtures and equipment of the Company;
- Sales or assignment of fictitious or misrepresented assets;
- Utilizing company funds for personal purposes.