Whistle Blower Policy_ Speak Up Guidelines

Document Number:	PP1038
Effective Date:	May 2023
Endorsed By: Audit and Risk Committee (May 2023)	Approved By: Board of Directors (May 2023)

REVISION LIST

Version	Date	Description
1.0	May 2023	First Version – Speak up guidelines

Whistle Blow- Speak Up Guidelines

- **Raising a Concern**

- **What should you report?**

a) When raising a Concern or making a report of fraud or misconduct, the following topics are subject matters typically raised through whistleblowing channels.
b) This list, however, is not exhaustive. If you believe that you have witnessed or suspected unethical, illegal, or unacceptable workplace conduct, you have an obligation to raise the Concern to Agthia.
c) You do not have to have detailed and exhaustive evidence of the wrongdoing and, in fact, Agthia does not want you to investigate it on your own.
d) Instead, Agthia expects you to raise the Concern in good faith in the designated platforms, providing any supporting evidence you have, so that it can be examined and remedied in a timely fashion.

- ✓ **Fraud**

a) Fraud is a broad concept that refers generally to any intentional act committed to secure an unfair or unlawful gain.
b) The Abu Dhabi Accountability Authority (ADAA) defines Fraud as follows:

- ✓ **Asset Misappropriation:** assets are misappropriated either directly or indirectly for the Stakeholder's benefit. Although any tangible assets can be misappropriated, certain assets like cash and a company's information are more susceptible to theft and misappropriation than others.

- ✓ **Fraudulent Statements**: fraudulent statements are statements (financial or otherwise) that bring a direct or indirect financial benefit to the Stakeholder. "Fraudulent statements" fall into two categories: fraudulent financial statements and all others. Examples of potential misstatement of Agthia financial statements could include improper cash flow projections and financial budgets, improper revenue recognition, overstatement of assets or understatement of liabilities.

- ✓ **Corruption:** when a Stakeholder breaches Agthia's trust in performing official duties on Agthia's behalf. This may include receiving Kickbacks from suppliers and paying bribes to public officials and commercial organizations.

- ✓ **Misconduct or Unethical Activities**

a) Misconduct and unethical activities are breaches of internal company policies and procedures, or other activities that involve potentially illegal or unethical conduct or threaten to harm Agthia's reputation and ability to conduct business in the marketplace.

- ✓ **Breach of Laws and Regulations**

    a. Any violations of law and government regulations applicable to Agthia or any other suspected irregularities should also be reported.
    (Refer to Appendix 1 for examples of potential Concerns and Breaches)

- **Information required for Investigation.**

    a. To facilitate Agthia's Investigation into a report submitted by you, you should provide as much detail as possible.
    b. For example, such information (although not mandatory to provide) would include:

- Your name, position and contact details (if you wish, however, you may decide to remain anonymous).
- The details and nature of the Concern.
- Full name and position the person(s) allegedly involved.
- Related documents, evidence, witnesses, and the location of any other information that would assist Agthia in investigating the Concern.

- **Reporting in good faith**

a) Agthia expects Stakeholders to report a Concern in good faith and will not tolerate intentionally false reports or reports made in malice. Making a report in good faith means you will be protected against retaliation; your report will be kept confidential as well as anonymous if you request so. Further details on the protections provided to Whistle-blowers who report in good faith are discussed in sections 5 and 6 of this Policy.
b) If a Stakeholder reports a Concern that he/she knows or reasonably should know to be false, he/she will be subject to disciplinary action as stated in section 9 of this Policy. Further, false reporting may have legal repercussions leading to civil or criminal prosecution.

- **How should you report?**

a) You should promptly report any suspected or potential wrongdoing you reasonably believe has taken place, is taking place, or will take place.
b) There are several channels through which you may report a Concern under this Policy. When deciding which channel to use, consideration should be given to the nature of the Concern, the individuals involved, and the Stakeholder's comfort level.
c) If reasonable grounds exist, promptly report the information through the appropriate channel, as listed below, however:
    - ensure that only those who need to know are informed.
    - do not alert people who may possibly be involved.
    - ensure that any notes and other evidence are handled carefully and kept secure.
d) The following channels of reporting should be considered by Employees:

✓ Employee's immediate manager or supervisor – Concerns can be escalated to the employee's immediate manager or supervisor. This is the primary channel of contact, which should be used by the Stakeholders if possible.
✓ The employee's Head of Department – If the employee does not feel comfortable escalating a Concern to their immediate manager or supervisor, or if they believe their manager or supervisor is involved – Concerns can be escalated to the relevant Head of Department.
✓ Head of Compliance – If the employee does not feel comfortable escalating a Concern to the Head of Department, or if the employee believes the Head of Department is involved – Concerns can be escalated to the Head of Compliance through the compliance mailbox (compliance@agthia.com)
✓ Through the independent whistleblowing channels provided by Agthia's external service provider as mentioned in Appendix 6 of the Policy
✓ Stakeholders other than employees can also escalate Concerns to the Head of Compliance using the same mailbox and/or Whistleblowing channels which are additionally explained on Agthia's webpage.
✓ If any Stakeholder does not feel comfortable escalating a Concern to the Head of Compliance or CVC, or if they believe the Head of Compliance and CVC members are involved – Concerns can be escalated to Audit & Risk Committee.

- **What happens after you report a Concern?**

    a. Concerns received through the Whistle-blower channels will be acknowledged unless the Whistle-blower has not provided their contact details.
    b. If any Concern is received by immediate managers/supervisors/departmental heads and if the concern is related to employee grievances, they should try to resolve as much as possible, however, if they are unable to resolve the matter, it is their responsibility to report the Concern to through whistle-blower channel and if the cases are related to the allegations they should not attempt to resolve or investigate by themselves, instead, they should report through normal whistle-blower channel.
    c. Once a Concern is received, it will be investigated fairly and confidentially in accordance with Section 7 of this Policy. If the whistle-blower has included their contact details upon raising their Concern, the Investigator may in certain situations reach out to them to obtain additional clarifications regarding the raised Concern.
    d. In addition to an acknowledgment of receipt, a Whistle-blower may also receive, if requested, general information on the progress and closing of the Investigation and its outcome, unless giving such feedback would be detrimental to the Investigation. You may refer to Section 7 for details on the Investigation process.

- **Anonymity and confidentiality**

    a. Agthia encourages all Stakeholders to report any Concern directly and openly as per Section 4.2 of this Policy. It is possible to report a Concern anonymously, however, anonymous reporting may make an Investigation more complex and may prevent appropriate action from being taken.
    b. Whether anonymous or not, all Concerns raised will be handled in a confidential manner. Confidentiality will be fully maintained possible, consistent with the need to conduct an adequate Investigation of the Concern and to implement any subsequent corrective and/or remedial measures.
    c. Stakeholders reporting Concerns via this Policy shall avoid any form of external or internal publicity relating to the Concern(s) they intend to report or have previously reported, unless required to do so by law.

- **Protection of the Whistle-blower**

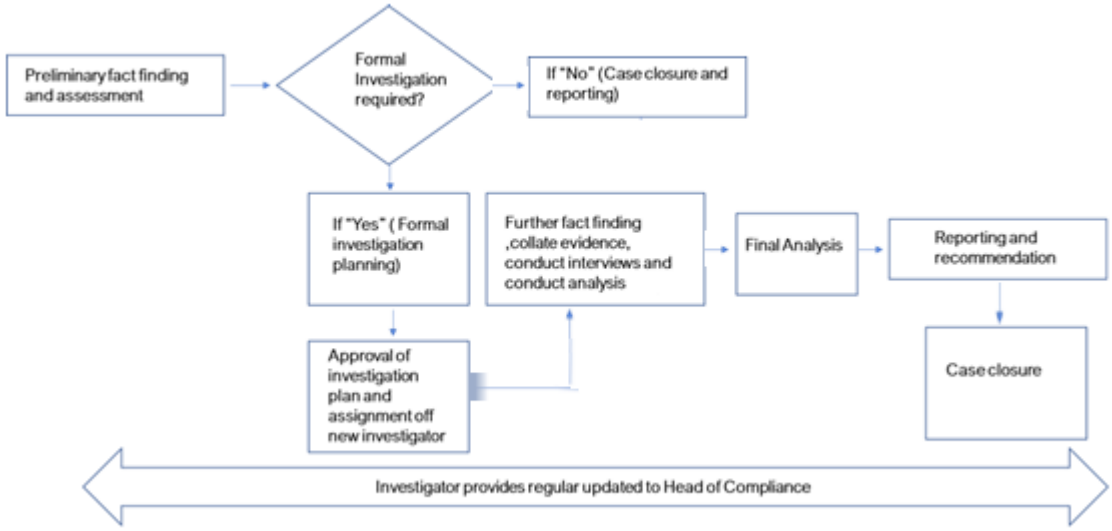
    a. Any Whistle-blower who reports a Concern, in good faith i.e. they have a reasonable basis to believe their Concern to be true, will be afforded protection for such reporting. This protection means that Agthia will not discharge, demote, suspend, threaten, harass or in any manner discriminate against the Whistle-blower in the terms and conditions of their employment or contract at/with Agthia for raising a Concern or cooperating with an Investigation under this Policy.
    b. Agthia does not tolerate any form of threat, retaliation, or other actions against a Whistle-blower who has made or assisted in the reporting a Concern. Any such threat, retaliation, or other action should immediately be reported to the Head of Compliance or others as per Section 4.2 of this Policy.

- **Investigation procedures**

    - **Overview of investigation process**
        - **Preliminary assessment**

a. Once a Case is reported through any of Agthia's speak-up channels mentioned in section 4.3 (d) of the Guidelines, the Case must be registered in the Case Register and assessed by Agthia Compliance. In case of any allegations raised to the attention of line management, it is the responsibility of those managers to involve Agthia Compliance as soon as they become aware of such an issue (without attempting to investigate it on their own).
b. The goal of the preliminary assessment is to determine if the allegations mentioned warrant an investigation or any other form of follow-up. While conducting this step, Agthia Compliance may involve other departments as appropriate to reach a conclusion or approach selected employees / third parties as deemed appropriate.
c. The preliminary assessment is generally an exploratory review of the allegations raised which consists of:
    - Reviewing and analysing the information/documentation presented by the complainant to determine the associated risks and repercussions of the allegations (if they were to be true)
    - Reaching out to the complainant (if necessary) to obtain additional information/clarification related to the raised allegations.
d. During the preliminary assessment phase, the following parameters should be considered in addition to the review of the provided information by the complainant:
    - Magnitude and severity of reported allegations
    - Significance and impact of allegations if they were found true, including the seniority and number of employees involved, potential liability for Agthia, and potential implications for commercial operations.
    - Type of reported allegation (e.g., corruption, bribery, theft)
    - If the case is a cross-border or multi-office investigation, the relevant jurisdictions pertinent to the misconduct.
    - Limitations of the investigation procedures for the presented allegations Whether an internal investigation is in the best interests of the company and its employees.
    - Whether an investigation is required by any specific laws or regulations
e. Allegations related to IT security should be handled by Agthia Cybersecurity in coordination with Agthia Compliance
f. A Case triage chart is included in Appendix 1.
g. The head of the compliance will escalate to the CVC immediately upon concluding preliminary screening of any allegations related to Agthia raised through speak-up channels, along with Agthia Compliance's recommendation concerning opening an investigation (or lack thereof). Upon receiving this information, the chairman will:
    - Validate Agthia Compliance conclusion on opening the investigation,
    - Advise on any required reporting to authorities (and the Agthia personnel responsible for this activity),
    - Decide on the creation of the Investigation Panel and its members (for Cases subject to an investigation).
h. If the Case does not warrant an investigation based on the preliminary assessment, the Case is closed in the Case Register with an appropriate justification provided as to why no investigation was conducted into the mentioned allegations.
i. If the Case does warrant an investigation, Agthia Compliance documents this fact in the Case Register and engages in stage 1 of the process as described below.
j. Investigations must be initiated within thirty (30) days of the Case being reported or otherwise detected.

A high-level summary of the investigation process is outlined below:



Stage 1: Planning the investigation.

a. Once the investigation initiation decision has been taken, Agthia Compliance will outline an investigation plan. Typically, the investigation plan includes:
   - Listing of specific Case allegations.
   - Anticipated activities to be performed in relation to each of the allegations.
   - List of initially anticipated interviews and relevant custodians.
   - The collection; preservation (including from back-up servers); and review of documents.
   - Potential risks (if any) which may hinder the investigation.
   - Assign investigators (including third parties/consultants if any).
   - Anticipated precautionary measures, including potential suspension of the employee if necessary, and suspension of discretionary bonus payments, salary increases, and promotions.
   - Anticipated timeline of the investigation.

b. Given that each investigation is different, it is challenging to set a specified time to complete each investigation (regardless of the Case category). Therefore, each investigation plan should include a detailed and realistic timeline for how long the investigation is expected to take, keeping in mind the time limits set by

the applicable laws. The investigation plan should be recorded in writing and kept on the investigation file.

c. At any point of the investigation Agthia Compliance may also decide to engage external consultants as appropriate for a given Case. The onboarding of such consultants will follow applicable Agthia policies & procedures.

Stage 2: Conducting the investigation.

a. When commencing the investigation, the investigators should take a hypothesis-based approach. This approach includes developing a theory of what may have occurred based on the preliminary assessment, testing the theory against readily available and newly identified information, and refining the theory as needed to reach a final opinion on whether the allegations mentioned in a Case have been proven, unproven, partially proven, or unfounded.
b. When conducting investigations into Cases, there is a possibility that the matter may eventually result in legal proceedings (e.g., a case raised by the company against the accused in criminal court). As such, it is crucial to notify, include, update, and refer to Agthia's Legal function for their legal opinion on matters related to the Case and respective investigation findings when conducting investigations.
c. Prior to commencing the investigation into a Case, the investigators, in cooperation with the Investigation Panel, should also consider whether it is necessary to temporarily suspend the accused employee to safeguard the efficacy of the investigation. This should however be discussed with both the legal and human capital functions beforehand (and any respective government authorities if necessary).
d. In cases where employees are temporarily suspended to conduct the investigation, the maximum period of suspension should be in line with local legislation. During this time, suspended employees are entitled to receive 50% of their usual salary. Wherever possible, all investigations where the subject is suspended should be completed within the thirty-day window. If the investigation finds no evidence of wrongdoing, the employee is entitled to receive the full sum of pay deducted during their suspension. If the investigation is criminal and is referred to the competent authority, wages may be suspended for the duration of the investigation.
e. The investigators need to ensure that during the investigation, for any employee who was accused of wrongdoing:
    - The employee has been appropriately notified in writing of the allegations against them. This notification can be affected through the written minutes of the employee interview; however, the accusation must be made, and the disciplinary process initiated within thirty (30) days of the offense being detected.
    - The employee has been given an opportunity to comment on the allegations.
    - The Investigator has investigated any defence provided by the employee in respect of the allegations.
    - The employee defence and evidence in support are recorded in the final investigation report.

- **Gathering and analysing evidence**

a. Based on the allegations mentioned in the Case, investigators will seek to gather and review a high volume of relevant evidence, whether physical or electronic in nature (e.g., policies, procedures, emails, contracts, purchase orders, access logs, CCTV footage, media storage devices, company laptops etc.). To ensure the

adequacy of the investigation, it is essential to properly handle and store any evidence gathered throughout the course of the investigation.

b. The relevant department (IT, HR, etc) should provide the information requested by investigator in max 24 hours of request.
c. Common principles when handling evidence of any kind (i.e., physical, or electronic) is to:
    - Seek to acquire the original piece of evidence as soon as its existence is identified to prevent tampering of any form.
    - Ensure the original pieces of evidence collected are properly and safely stored.
    - Establish an appropriate referencing system for each piece of evidence.
    - Document the timing and source from which the evidence was collected.
    - Only allow authorized and experienced investigators to access/review the original documents, who should administer the highest level of care and diligence while doing so to preserve the chain of custody; and
    - Whenever possible, establish a logging system to show who had accessed and/or copied any pieces of evidence relevant to the investigation.
    - The evidence and relevant documentation should be preserved for 8 years. The document preservation responsibility will be with compliance. All investigators should send the documents to compliance for storage and archival.
d. When analyzing any pieces of evidence, if possible, investigators should create and analyse copies of the original pieces of evidence to avoid mismanagement of evidence. Any copies of original pieces of evidence should be treated with the same level of security as the original pieces of evidence. The analysis must also be properly documented in well-referenced and safeguarded working papers.
e. At no point in time throughout the course of the investigation should the investigators create scenarios to capture the accused employees in the act of committing the allegations mentioned in the Case (i.e. create scenarios to obtain evidence). This term is referred to as “entrapment” and is not permissible. Investigators should also not conduct any form of covert surveillance or recording of the suspect, irrespective of whether the circumstances have occurred without interference. In all cases where employees may be subject to monitoring or recording, they must be informed in advance, although investigators need not disclose the purpose of the monitoring/surveillance.

- **Data access and privacy**

a. Whenever access to an employee’s electronic records (e.g., emails) or human capital records is required as part of the investigation, it is mandatory for the investigators to consult with Agthia’s Legal and Human Capital prior to obtaining any such information.
b. The investigators must always respect and protect the privacy rights of individuals involved in the investigation. This includes the reporter of the Case, witnesses, subject matter experts, and the subject(s) of the investigation.
c. Investigators cannot compel employees to submit their personal devices for interrogation. Agthia has the right to access and forensically examine data held on company-owned devices. If investigators suspect that significant evidence is held on an employee’s personally owned device, they may only examine this data with the written consent of the employee. Access to a personal device may only be compelled by the local legal authority such as court.

- **Interviews**

a. After determining whether an individual should be interviewed as part of the broader investigation, there are three phases of the interview process.
b. The first phase is preparing for an interview. During this phase, the investigators must:
    - Prepare the appropriate questions to ask during the interview.
    - Ensure the proper supporting documents (if any) are made readily available and accessible for the interviewers to reference and present to the interviewee throughout the course of the interview; and
    - Ensure that the interview will be conducted in line with the applicable laws.
c. The second phase is organizing and conducting the interview. During this phase, the investigators should ensure:
    - Booking an ample (but realistic) amount of time to fully conduct the interview.
    - Whenever possible, arrange for an in-person interview with the individual in question.
    - (In particular in case of potential suspects) at a location which they feel comfortable in The presence of at least two interviewers during the interview, with at least one of the interviewers being the same gender as the interviewee if possible.
    - Starting the interview by informing the interviewee of the reasons behind the interview and applicable confidentiality protocols.
    - Optionally, recording the interview upon informing the interviewee of this fact prior to commencing the interview. If the employee objects to being recorded, the interviewer may proceed with the interview but must not record any video or audio during the process.
    - The interview is conducted in a respectable, objective, and professional manner to not give a sense of intimidation or interrogation to the interviewee.
    - If the interviewee is not fluent or comfortable in the language of the investigation, a translator should be offered to assist. The translator will only work as a language translator. He may not have similar access to the records as an investigator. The translator will need to sign NDA and need to keep information related to the investigation confidential.
d. The third phase is documenting the discussion during the interview (please also refer to Appendix 5 for a suggested template of interview minutes). In this phase, the investigators should:
    - Document the interview in the form of (verbatim) minutes, which reflect the questions asked and the exact given responses, using interviewees' own words. Where a translator has been provided, verbatim minutes must also include the original language of the interviewee. The employee may confirm the minutes via email provided they clearly indicate the record they are approving of.
    - Ensure that the minutes are confirmed (signed) by the interviewee, who should additionally confirm in writing that:
        - The minutes reflect the interview correctly.
        - The statements were made voluntarily and not under duress.
        - They read and understood what had been documented in the minutes.
    - Whenever possible, obtain interviewee's confirmation of the minutes at the end of the interview. This step is crucial in case of interviews with potential suspects.

- Where an interviewee or witness is asked to sign a statement of truth or the minutes of the meeting, it should also be countersigned by all of the other attendees present at the interview.

- **Investigation notifications**

a. In consultation with the Investigation Panel, the investigators should:

- ensure that compliance with applicable laws is ensured in terms of deadlines for notifying any investigated employees (e.g., within a specific time period from discovering the incident);
- decide when to inform any relevant authorities (e.g., Police) of the investigation; and
- determine whether they are required to disclose any Cases and/or ongoing investigations within Agthia to any other Government Bodies (e.g., Abu Dhabi Accountability Authority).

Stage 3: Concluding and reporting the investigation.

a. Once all key steps of the investigation plan have been completed by the investigators should provide a draft report to the Investigation Panel (please refer to Appendix 3 for a suggested template of a report). The report should be objective, factual, clear, and concise and include (at a minimum) the following information:
   - Background of the Case and listing of allegations.
   - Scope, objectives, and methodology of the investigation.
   - List of personnel involved in the investigation and with knowledge of the Case.
   - The list of documents/records/reports verified.
   - Assessed the risk level of the case (in line with Appendix 2);
   - An executive summary of the investigation.
   - Detailed findings of the investigation.
   - Any circumstances which might have hindered the investigation.
   - Conclusion.
   - Recommended action plans, including and remediation action.
   - List of key activities performed during the investigation.
   - List of interviews conducted throughout the course of the investigation.
   - If any reporting obligations have been triggered.

b. The Investigation Panel, as part of the ongoing investigation, should review the draft report and guide the investigators in terms of steps required to close the investigation. This should include:
   - Any additional procedures required within the investigation.
   - Reconfirmation of the recommended action plans.
   - Any next steps and additional reporting protocols.

c. Upon fulfilling the additionally recommended steps, the investigators should reconfirm the outcomes with the Investigation Panel. Once confirmed, the investigators should issue the final report to the Investigation Panel and close the Case in the Case Register (along with any additionally recommended actions).
   - If the investigation found the Case allegations to be either proven or partially proven, the investigation report should include the proposed action plans to mitigate the current situation, prevent, and detect similar Cases from occurring in the future.
   - If the investigation found the Case allegations to be unproven, the investigation report.
   - should include what (if any) are the next steps following the investigation.

- If the allegations were deemed to be unfounded based on limitations throughout the course of the investigation, the investigators should outline such limitations in the investigation report.
- Upon receiving the final report, the Investigation Panel should recommend the disciplinary measures to be applied (if any) and coordinate with the appropriate functions within Agthia to execute those steps as required within the applicable laws. If it has been established that there is sufficient evidence confirming the truthfulness of the allegations mentioned in the Case, the accused individual(s) must be notified of the investigation results as soon as professionally possible (within the applicable legal framework). Any disciplinary action must be taken against the employee within sixty (60) days of completing the investigation and establishing the allegations.

d. The Investigation Panel should also ensure the appropriate notification of any authorities (e.g., ADAA or the Police) as required. Also, the investigation panel will make sure that insurance companies are informed in time.

➢ **Role of the subject of the Investigation**

a. An individual who is the subject of an Investigation or a witness to misconduct that is the subject of an Investigation, is required to cooperate with the Investigator when his/her assistance, or the assistance of any person under his/her supervision, is sought with respect to any Investigation.

b. This means that the individual should:

✓ Make themself, any persons whom he/she supervises, and any relevant documents/records available to the Investigator or any other person who is assisting with an Investigation.

✓ Failure to cooperate in an Investigation is subject to disciplinary action up to and including termination.

✓ Not destroy or alter documents which may be relevant to the Investigation, intimidate possible witnesses or interfere otherwise in the Investigation.

✓ Answer questions truthfully.

✓ Volunteer any information in good faith that may assist with an Investigation.

✓ Keep confidential any information that he/she receive as part of an Investigation, including the existence of the Investigation, the persons involved and the factual issues.

✓ Not make recordings of interviews conducted in person or via telephone or videoconference without the prior written consent of the Head of Compliance. The Head of Compliance may grant an Investigator approval to conduct the compliance-related interviews in person or via telephone or videoconference or to record an interview where appropriate. Prior to commencement of a recorded interview, interviewee will be notified and will be required to provide consent to being recorded.

c. Any communications made using an Agthia computer, telephone, mobile device, SIM card, or other electronic resource, and the information stored on them, are Agthia property and, where permitted by law, may be searched, or monitored without prior notice or consent, including during an Investigation.

- **Reporting**

a. The Head of Compliance shall provide a statistical summary of reported Concerns, Investigations, and conclusions of such Investigations to the ARC. The Head of Compliance may immediately report Breaches to the ARC upon becoming aware of them depending on the severity of the issue at hand.

b. In case of a Concern involving a member of the Board, the ARC and the Head of Compliance shall ensure an appropriate reporting process is in place.
The diagram below depicts the Investigation and reporting process and the Stakeholders involved at each stage.

- **Disciplinary actions**

a. Disciplinary actions will be implemented in line with the Agthia's Code of Conduct and HR Policies.
b. Such disciplinary actions may include, amongst others:
   - Coaching
   - Verbal warning
   - Written warning
   - Final Written Warning
   - Suspension and/or termination.

- **Staff training and awareness**

a. Agthia will increase employee awareness on its Whistleblowing Policy by conducting awareness sessions, issuing e-mail communications, or conducting any other necessary campaigns across the company.
b. The Head of Compliance will be responsible for ensuring that the Policy is communicated to all Agthia employees and properly shared with Agthia's Subsidiaries.
c. If needed and as required, the Head of Compliance shall arrange training for employees on how to detect and prevent wrongful behaviour and how to comply with the Policy.

➢ **Record retention**

a. The Head of Compliance shall maintain a log of all Concerns received and track their receipt, Investigation, and resolution. He/she shall also maintain copies of the periodic summary reports submitted to the ARC. All records shall be maintained in accordance with applicable legal and regulatory requirements.
b. Internal and external Investigators engaged by the Head of Compliance and/or ARC, such as Internal Audit, HR Function, Legal Function, and external forensic investigators (including law firms or consultants), shall send appropriate records of

all Investigations in accordance with applicable legal and regulatory requirements to compliance department for retention.

❖ Appendix-1 Potential concerns or breaches

#	Category	Description
1	Abuse or harassment in the workplace	Any form of abuse or harassment, in any company workplace, toward employees, contractors, suppliers, customers or others.
2	Breaches of Gifts & Entertainment policies	Failure to adhere to Agthia policies in respect to the giving or receiving of gifts and entertainment. Instances in which the recipient of the gift or entertainment is a government official or is in any way related to business with governments in any location that BP operates will always be a significant incident and must be escalated.
3	Breaches of Intellectual Property and copyright of others	Dishonest and inadvertent disclosure, and misuse, of confidential intellectual property and protected information of Agthia and others.
4	Breaches of trade restrictions, export controls and sanctions	Any Breaches on restrictions on exports and dealings with certain restricted countries or persons as per UAE and international regulations impacting Agthia.
5	Competition & anti-trust violations	Any potential Breaches of Competition/anti-trust legislation, being laws that promote or protect free and fair competition around the world. Anti-competitive behaviour includes talking with or exchanging information with competitors to: □ Fix prices □ Fix terms □ Divide up customers, markets, or territories. □ Limit production, including agreements to shut down capacity. □ Rig competitive bidding processes (i.e., agreeing to submit sham bids).
6	Conflicts of interest	Failure to comply with the Agthia Code of Conduct in respect of interests that could interfere or be perceived as interfering with the employee's professional responsibilities at Agthia.
7	Data theft; breaches of and employee confidentiality	Deliberate abuse or negligence resulting in theft, disclosure, publishing, improper privacy, insider trading use or any other type of violation of information confidentiality requirements at Agthia (including confidential information, insider information concerns and/or personal data concerns).
8	Failure to protect Agthia's assets	Misuse or waste of Agthia's assets including property, time, proprietary information, corporate opportunities, and company funds, as well as personal company equipment where the suspected Breach does not fall under the definition of Fraud. Examples include:

#	Category	Description
		✓ Theft (where a deliberate deception is involved in the act, such as falsification of documents, it would be classified as Fraud). ✓ Not taking reasonable care with Agthia assets. ✓ Abuse of company assets for personal use. ✓ Undertaking an unreasonable number of personal activities during company time (dishonest recording of hours worked would fall under the definition of Fraud). ✓ Theft or failure to take reasonable care to protect Agthia's intellectual property and confidential information.
9	Fraud	Fraud can be generally defined as any behaviour whereby one party intends to gain a dishonest advantage over another or to cause loss to another or to expose another to a risk of loss. Fraud covers any deliberate deception that generally involves the following: Dishonest manipulation or falsification of company records or accounts. - Dishonestly making a false representation that is untrue or misleading and the person making the representation knows it is, or might be, untrue or misleading. The representation may be express or implied. - Dishonestly failing to disclose information which the person is under a legal duty to disclose. - Dishonest abuse of position in which a person is expected to safeguard or not act against the financial interests of another person. - Examples of Fraud include: - Financial statement Fraud - recording fictitious revenues, manipulation of timing of transactions, concealing liabilities, or expenses, incorrect or misleading disclosures or asset valuations. - Conflicts of interest / procurement Fraud - collusion with suppliers, collusive bidding, false invoicing schemes, personal purchases with company funds. - Payroll Fraud - ghost employees, falsified hours or salaries, sales commission falsifications. - Expenses schemes - overstated and/or fictitious expense claims, over- purchasing, claiming for personal expenses. - Theft involving manipulation of records - Cheque tampering / skimming schemes - Other falsifications
10	Improper digital systems use and security Breaches	Misuse of Agthia's digital systems for personal or unauthorised use and deliberate Breaches of Agthia's digital security guidelines.

#	Category	Description
11	Inaccurate or incomplete data, records, reporting or accounting	Deliberate inaccurate recording of data can include financial as well as non- financial data. This class of Breach will generally be classed as Fraud.
12	Money Laundering	Money laundering can include any action (including use, transfer, or retention) in relation to the proceeds of crime (including cash and other property) of any crime, however minor.
13	Unfair treatment or unequal employment opportunity	Any unfair treatment of employees or contractors, including: ○ discrimination in the form of race, colour, region, gender, age, national origin, marital status, or disability ○ recruitment selection, development, and advancement not based on merit. ○ not adhering to applicable labour and employment laws

❖ Appendix 2 – Case triage rules

Allegation Type	Responsible Function
Alleged violations of the Code of Business Conduct, including but not limited to: assault, asset misappropriation, attendance issues, bribery or corruption, bullying, conflicts of interest, discrimination, fraud, harassment, intentional breach of company policies, insider trading, misuse or abuse of company resources, money laundering, nepotism, retaliation, sexual harassment, substance abuse, theft, unethical & unprofessional conduct.	Compliance Function
Employee Grievances, with no elements of alleged violation of the Code of Business Conduct, which the reporting employee believes to be either unfair, incorrect, or in violation of their agreement with Agthia. Examples include (but are not limited to): employee assessments, promotions, salary disputes, terms and conditions of employment (working hours, workload, annual leave days, compensation etc.)	Human Capital/ Compliance Function
IT Security issues, including any data leakage. incidents within Agthia's information technology systems.	IT Security/ Cyber Security/ Compliance Function

❖ Appendix 3 – Case risk levels

Level	Criteria
High	Potential financial exposure to company in excess of AED 500,000 National or International, long-term media coverage Widespread employee and senior management impact Probable breach of external laws or regulations leading to litigation Probable sanctions and/or financial penalties from authorities Allegations related to C-level employees (e.g., Chief)
Medium	Potential financial exposure to company between AED 100,000 and AED 500,000 Short-term, local, or national media coverage Potential employee morale problems Potential breach of external laws or regulations Potential sanctions and/or financial penalties from authorities
Low	Potential financial loss to company is less than or equal to AED 100,000 No media coverage Isolated employee dissatisfaction No breach of external laws or regulations No expected sanctions and/or financial penalties from authorities

❖ Appendix 4 – Template investigation report

Company name
Internal Investigation Report Date: _____
Title: [Project name or investigated area name]
Page 1
Background:
[Description of the circumstances triggering the investigation]
Listing of allegations:
[Summary of allegation[s] the form of a clear list in case of multiple allegations]
Compliance classification:
[Indication of Ethix360 primary and secondary allegation classification]
Risk:
[Assessed risk level as per Appendix 2 guidelines]
Investigation conclusion:
[Select from the following: Substantiated / Partly substantiated / Not substantiated / Inconclusive]
Executive summary:
[A few concise paragraphs with a high-level outcome of the investigation]
Page 2 and following pages
Detailed findings:
[Description of the findings, separate into several chapters addressing each accusation separately in case.
of multiple allegations]
Recommended action plans, including and remediation action.
[List of recommendations / SMART action plans, i.e., specific, measurable, achievable, responsibility (clearly
assigned), time-bound]
Appendices
1) Scope, objectives, and methodology of the investigation.
2) List of key activities performed during the investigation.

3) List of personnel involved in the investigation and with knowledge of the Case.
4) List of interviews conducted throughout the course of the investigation.
5) Any triggered reporting obligations (only if such circumstances appeared)
6) Any circumstances which might have hindered the investigation (only if such circumstances appeared).

❖ Appendix 5 – Template interview minutes

Company name: _____

Meeting minutes Date: _____

Interviewee: _____

Interviewers: _____

Interview introduction:

Interviewee informed of the reasons behind the interview at the start of the interview: YES □ NO
Interviewee informed of the applicable confidentiality protocols: YES □ NO □
Interview audio recorded: YES □ NO □

Verbatim minutes:
Questions: Answers:
Question 1 Answer 1
Question 2 Answer 2
[...] [...]

By signing these minutes, the Interviewee confirms that:
- The minutes reflect the interview correctly.
- The statements were made voluntarily and not under duress.
- The Interviewee read and understood what had been documented in the minutes.

❖ Appendix 6– Independent Whistleblowing Channels

Agthia has partnered with an external service provider, Ethix360, to provide a dedicated 24/7 reporting channel for all Agthia employees. The provided channels are:
- Webpage: https://agthia.ethix360ae.com
- All toll-free numbers have been activated. The numbers for the program are:

Egypt	+20 150 169 2051
Jordan	0800 23214
Kuwait	+965 2205 9283
Oman	800 74530
Saudi Arabia	800 850 0256
UAE	800 06512072