CPHCL

CPHCL WHISTLEBLOWING POLICY

General Principles applicable to the Group

CHAPTER 1. DEFINITIONS

In this Whistleblower Policy (hereinafter referred to as '**the WB Policy**'), the following terms shall have the meaning ascribed to them below, unless the context otherwise requires:

1.1 Alleged Perpetrator: means allegedly that person if identified or identifiable who has conducted the wrongdoing;

1.2 **Audit Committee**: means the Audit Committee of CPHCL (as defined hereunder);

1.3 **Group Company:** means anybody corporate which is CPHCL's subsidiary or parent company, or a subsidiary of CPHCL's parent company, and the term "Group" shall be construed accordingly;

1.4 **CPHCL:** means CPHCL Company Ltd (Malta Registration Number C257) - also referred to as '**the Company'**;

1.5 **Protected Disclosure:** Any and all disclosures that qualify for protection of the Whistleblower under the laws of the Relevant Jurisdiction;

1.6 **Relevant Jurisdiction:** the jurisdiction where the Group Company that employs the Whistleblower or the Whistleblower is providing a service to the Group Company is situated. In the circumstance that the Whistleblower is employed or provides a service in a jurisdiction where there is no protection of the Whistleblower legislation, in the jurisdiction where CPHCL head office is situated;

1.7 **Whistleblower:** Any CPHCL or Group Company employee, former employee, external worker, contractor, subcontractor, intern, trainee, outworker, or candidate for employment who makes a disclosure to a Whistleblower Reporting Unit for the reporting of irregularities, as the case may be, whether it qualifies as a Protected Disclosure or not under the law of the Relevant Jurisdiction;

1.8 **Whistleblower Reports Unit:** hereinafter referred to as "WRU", is a unit made up of: the chairman of the Audit Committee, the Group CEO, and the Company Secretary;

CHAPTER 2. PURPOSE

2.1 The present WB Policy has been established based on the Directive (EU) 2019/1937 on the protection of persons who report breaches of European Union (the "Union") law (the "Directive") that creates a framework for persons who acquired information on certain breaches in connection with their work-related activities and serves to set **minimum standards and principles** for the protection of persons reporting said breaches. Each Group Company is additionally subject to and solely responsible for compliance with the laws in its own Relevant Jurisdiction. Where the laws in the Relevant Jurisdiction exceed or contradict the principles in this WB Policy, the law in the Relevant Jurisdiction shall take precedence. CPHCL shall not be held liable in the event that a Group Company fails to observe the laws in its Relevant Jurisdiction.

2.2 This WB Policy is subject to potential alterations and adjustments, taking into account legislative amendments and their respective implementations into the Relevant Law. Employees shall be kept informed of these changes.

2.3 The principal objective behind this policy is to provide a Whistleblower with the possibility to report a misconduct through an internal reporting channel that safeguards the Whistleblower's identity.

2.4 This policy is applicable to all personnel within the Group, both part-time and full-time, encompassing contractors or subcontractors engaged to perform work or provide a service, external workers, former employees, trainees or interns, and candidates for employment, solely when information about suspected improper conduct has arisen during the recruitment process or during the pre-contractual negotiation phase.

2.5 The protection granted to the Whistleblower's identity ensures that reporting of misconduct can take place without fear of facing any form of retaliation.

2.6 Simultaneously, the Group is given the chance to examine and carry out appropriate measures to address the potential cases of misconduct.

CHAPTER 3. PROTECTED DISCLOSURE

3.1 This WB Policy covers Protected Disclosures made concerning specific cases that have occurred, are possibly currently occurring, or are likely to occur in the future, (collectively referred to herein as '**Misconduct**'). Under this policy, a 'Protected Disclosure' is deemed to encompass any disclosure that falls within or is susceptible to falling within the scope of one of the following situations:

a) a person has failed, is failing or is likely to fail to comply with any legal obligation to which he/she is subject; or
b) the health or safety of any individual has been, is being or is likely to be endangered; or
c) the environment has been, is being or is likely to be damaged; or
d) a corrupt practice has occurred or is likely to occur or to have occurred; or
e) a criminal offence has been committed, is being committed or is likely to be committed; or
f) a miscarriage of justice has occurred, is occurring or is likely to occur; or
g) bribery has occurred, or is likely to occur or to have occurred; or
h) a person has failed, is failing or is likely to fail to comply with any legal obligation on public procurement to which he/she is subject; or
i) a person has failed, is failing or is likely to fail to comply with laws on financial services, products and markets, and prevention of money laundering and terrorist financing; or
j) a person has failed, is failing or is likely to fail to comply with product safety and compliance law; or
k) a person has failed, is failing or is likely to fail in ensuring transport safety; or
l) person has failed, is failing or is likely to fail in ensuring radiation protection and nuclear safety; or
m) a person has failed, is failing or likely to fail in ensuring a food and feed safety, animal health and welfare; or
n) a person has failed, is failing or is likely to fail to comply with any legal obligation on consumer protection to which he/she is subject; or

o) a person has failed, is failing or is likely to fail to comply with any legal obligation on protection of privacy and personal data, and security of network and information systems to which he/she is subject; or
p) a breach relating to fraud and any other illegal activities affecting the financial interests of the European Union or a Relevant Jurisdiction has occurred or is likely to occur or to have occurred; or
q) a breach relating to the internal market[1] including breaches of European Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law has occurred or is likely to occur or to have occurred or a breach of any other similar laws in a Relevant Jurisdiction; or
r) information tending to show any matter falling within any one (1) of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

For the avoidance of doubt, if a person is uncertain as to whether a breach would fall within the terms of this WB Policy or otherwise, such breaches should be reported, nonetheless. In the event the reported matters are later found to be false or inaccurate, one must assess whether the Whistleblower had legitimate reasons to believe the report to be true. In such case the Whistleblower shall not be held criminally liable.

3.2 This policy is not intended to:

i Question the financial or commercial decisions made by the Group;

ii Reconsider any matters already investigated under other policies or procedures issued by the Group, unless new facts or evidence arise suggesting that the issue should be reinvestigated.

3.3 Any matter not meeting the requirements outlined in this chapter should be treated as a Grievance, rather than a Protected Disclosure, and the Group is not obliged to initiate investigations or maintain the Whistleblower's identity confidentiality. The determination of whether the reported acts are considered a Protected Disclosure under this rests with the WRU.

3.4 The WRU may seek legal advice to ascertain whether the reported facts constitute a crime or violation of legal obligations under the legislation of the Relevant Jurisdiction where the alleged acts occurred, as long as the confidentiality of the Whistleblower is preserved.

3.5 Depending on the complexity and nature of the case, the WRU may engage the assistance of internal or external experts, provided that the identity of the Whistleblower is maintained.

CHAPTER 4. ANONYMITY AND DATA PROTECTION

4.1 Confidentiality

4.1.1 CPHCL ensures to protect the **confidentiality** of the identity of the Whistleblower, as well as of any third party mentioned in the report. CPHCL further ensures that non-authorized staff members shall not have access to such reports and that those who have access thereto are bound by a duty of confidentiality.

[1] The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured.

4.1.2 Without the explicit consent of the Whistleblower or at the request of the competent authority, as required by law, the identity of the Whistleblower (or any other information from which the identity of the Whistleblower may directly or indirectly be deduced) is not to be disclosed to anyone other than the authorised staff members competent to receive or follow up on reports.

4.1.3 The Whistleblower is to be informed when disclosure is mandated by law, unless doing so jeopardises the investigation into the disclosed matters. No disclosure shall be made in such a situation.

4.2 Personal Data

4.2.1 Any processing of personal data done in line with this WB Policy (including the sharing or transmitting of personal data by any Group Company and appropriate authorities must be compliant with:

i. Regulation (EU) 2016/679 of the European Parliament and of the Council, dated April 27, 2016, concerning the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**");

ii. Any applicable privacy laws in the Relevant Jurisdiction.

4.2.2 Personal information that is obviously unrelated to how a particular report will be handled must either not be collected or, if unintentionally gathered, must be promptly removed.

4.2.3 The pertinent information must be kept on file for at least five (5) years or, in cases where legal or administrative actions regarding the report are pending, for the duration of those actions, including any criminal ones.

CHAPTER 5. PROTECTION MEASURES

5.1 As long as the reporting was done in accordance with the guidelines outlined in this WB Policy and is based on information that the Whistleblower reasonably believed to be accurate at the time of the reporting, the Whistleblower will not be held accountable in civil, criminal, or disciplinary actions for making protected disclosures.

5.2 The Whistleblower will have access to support measures as necessary, including the following in particular:

i. the right to legal representation in any legal actions that may be brought up in relation to the reported issues;
ii. witness safety precautions in legal processes;
iii. adequate help from competent authorities if required.

5.3 A Whistleblower who has made a Protected Disclosure in accordance with this WB Policy is protected from any type of **occupational harm**, particularly in the following ways:

i suspension, layoff, termination, or similar actions;
ii a promotion being rescinded or delayed;
iii a change in the nature of the job, the location of the workplace, the pay, or the hours worked;

iv denial of training;
v a poor performance review or a bad employment reference;
vi the imposition or administration of any corrective action, censure, or other consequence, including a monetary fine;
vii coercion, fear-mongering, harassment, or exclusion;
viii unjust, derogatory, or discriminatory treatment;
ix failure to convert a temporary employment contract into a permanent one in cases when the employee had reasonable expectations of receiving a permanent job offer;
x the early termination or non-renewal of a temporary employment contract;
xi damage to a person's reputation, notably on social media, or financial loss, such as a reduction in revenue or loss of business;
xii blacklisting based on an informal or official agreement made by all parties in the industry or sector, which may mean that the person will no longer be able to work there in the future;
xiii early contract cancellation or termination for goods or services;
xiv revocation of a permission or licence;
xv recommendations to a psychiatrist or a doctor;
xvi facing disciplinary action, such as for violating confidentiality or ethics; and/or
xvii being subject to an employment or retirement term or condition that is changed or kept changed to the whistleblower's detriment;
xviii any disciplinary action taken against the whistleblower within two (2) years of the report's submission.

When carried out up to two (2) years following the Whistleblower's revelation, all such actions are presumed, until shown otherwise, to have been inspired by the report.

5.5 A Whistleblower who has made a Protected Disclosure in accordance with this WB Policy is protected from any form of retaliation. Retaliation includes all actions that result in the Whistleblower suffering patrimonial or non-patrimonial loss, including.

i. any behaviour that results in harm, loss, or damage; and/or
ii. victimisation, coercion, or harassment; or
iii. harm to one's career; and/or
iv. prosecution for making false charges under criminal laws; and/or
v. Court cases, criminal charges, or disciplinary actions.

CHAPTER 6. PROCEDURE TO DISCLOSE IDENTITY OF THE WHISTLEBLOWER

6.1 When the Whistleblower grants permission or desires his/her identity to be disclosed throughout the entire procedure, the Identity Disclosure Authorization Statement provided in **Annex I** must be completed and signed by the Whistleblower.

6.2 The Identity Disclosure Authorization Statement can be completed and signed before, during, or after the investigation procedure has been concluded.

6.3 The key steps in the whistleblowing procedure shall be the following:

i. Whistleblowing report is received;
ii. The WRU will acknowledge receipt of the report;
iii. Following this, the WRU will carry out an assessment on the accuracy of the allegations made, and revert to the Whistleblower;
iv. There may or may not be a physical meeting;
v. More information may be needed and requested from the Whistleblower;

vi. The WRU will follow up with the Whistleblower and provide feedback on what the decision taken has been.

This procedure may be modified as legislated in the Relevant Jurisdiction.

6.4 Any potential acts of retaliation arising from the disclosure of the Whistleblower's identity may be reported through the reporting channel established in this policy.

The Whistleblowing Reports Unit (WRU) of the Group is made up of the following persons:

The Chairman of the Audit Committee – Mr Joseph F.X. Zahra

The Group CEO – Mr Jean-Pierre Schembri

The Company Secretary – Mr Alfred Fabri

CPHCL

ANNEX I. IDENTITY DISCLOSURE AUTHORIZATION STATEMENT

I, _____ [Whistleblower's Name], identified by _____ [Type of Identification Document] number _____ [Identification Document Number], hereby expressly grant permission for my identity to be disclosed during and after the investigation process related to the disclosure submitted by me.

I am aware that my identity may be revealed to parties involved in the investigation, in order to facilitate the proper conduct of inquiries and ensure a fair process.

I understand that by providing my consent for the disclosure of my identity, this decision is irrevocable.

By signing this declaration, I am cognizant of the implications of disclosing my identity and confirm that I am making this decision voluntarily and informedly.

_____ _____

Whistleblower’s signature Date

CPHCL

ANNEX II:
MALTA ANNEX

(Procedures and Provisions applicable to entities within the Group established in MALTA)

The following provisions, which are additional to and form an integral part of the WB Policy, comply with the **Protection of the Whistleblower Act, Chapter 527 of the Laws of Malta**.

1. FILING & RECEIVING THE DISCLOSURE

1.1 Internal Disclosure

1.1.1 A Whistleblower wishing to file a disclosure shall do so through the internal reporting channel by completing the form reproduced below and submitting it directly and exclusively to the WRU by sending an email to the dedicated email address: whistleblower.cphcl@corinthia.com When filing the disclosure, the Whistleblower should aim to provide sufficiently detailed information for the purposes of enabling the WRU to gather an understanding of the alleged breach in question.

1.1.2 The report may be submitted in writing or orally. To that effect, a physical meeting or telephone call, on 99696858, may be scheduled with the Group CEO. A record of this meeting must be drawn up or, in the case of oral reporting, the call must be recorded. The report may also be made through a voice recording system.

1.1.3 Upon receipt of a disclosure, the WRU shall acknowledge the receipt of the report within seven (7) days of that receipt and shall then carry out an assessment on the accuracy of the allegations made in the report, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure, whilst keeping the Whistleblower informed of the progress of the assessment. When acknowledging receipt of the report, the WRU shall also inform the Whistleblower of the requirements, the competent authorities to assess the external reporting and the form and admissibility thereof.

1.1.4 Upon request by the Whistleblower, the WRU shall set up a physical meeting within a reasonable timeframe, which shall not exceed one (1) month from the date of acknowledgement of receipt.

1.1.5 The WRU may ask the Whistleblower to provide further information during the course of the investigation. All communications must be exchanged through a reporting system that provides for such communications to be made anonymously.

1.1.6 The WRU shall ensure to diligently follow-up on any disclosure filed by a Whistleblower and shall provide feedback on the outcome of the disclosure to the Whistleblower within a period not exceeding three (3) months from the date of the acknowledgement of receipt, or if no acknowledgement was sent to the Whistleblower, within a period not exceeding three (3) months from the expiry of the seven (7) day period after the report was made.

1.1.7 The Chairman of the WRU shall be the Head of the Audit Committee. Decisions of the WRU will only be valid if taken by a majority of the votes of all its members.

1.1.8 The Whistleblower may file an internal disclosure directly to the head, or deputy head of the Audit Committee if the Whistleblower has reasonable grounds to believe that the any person in the WRU is or may be involved in the alleged improper practice, or if the Whistleblower has reasonable grounds to believe that a person in the WRU is (by reason of any relationship or association with a person who is or may be involved in the improper practice alleged in the disclosure) not a person to whom it is appropriate to make the disclosure.

1.2 External Disclosure

1.2.1 The Whistleblower shall have the option of filing an external disclosure to the competent authorities listed in **Clause 1.3 below** (each, an "**External Reporting Channel**").

1.2.2 As explained above, this may be done after having first reported through internal reporting channels, or by directly reporting through applicable External Reporting Channels, that mainly concern cases in which the Whistleblower has reasonable grounds to believe that:

i. Those in charge of dealing with and handling reports are, or may be involved in the improper practice alleged in the disclosure; or

ii. Immediate reference to the authority is justified by the urgency of the matter to which the disclosure relates, or some other exceptional circumstance; or

iii. At the time when the external disclosure is made, the Whistleblower will be subjected to an occupational detriment by his/her employer if said Whistleblower makes an internal disclosure or face any other manifest risk of retaliation; or

iv. It is likely that evidence relating to the improper practice will be concealed or destroyed if he/she makes an internal disclosure; or

v. Although an internal disclosure has previously been made, the Whistleblower has not been informed on the status of the matter disclosed or it is reasonably evident to the Whistleblower that there has been no action or recommended action on the matter to which the disclosure relates within a reasonable time from the making of the disclosure.

1.2.3 Under the conditions outlined by the External Reporting Channels of each of these competent authorities, reporting will be permitted in writing, verbally, and, upon the Whistleblower's request, through the use of a physical meeting within a reasonable timeframe. The External Reporting Channels must permit the Whistleblower to maintain anonymity, much like the internal reporting channels.

1.2.4 After receiving a disclosure, the relevant authority indicated below must decide whether the disclosure is to be published publicly or otherwise. If the authority decides at its sole and absolute discretion that a disclosure should have remained internal, the Authority must give the Whistleblower written notice to that effect, within a reasonable amount of time. On the other hand, if the authority determines that a disclosure has been made properly, it is required to give the Whistleblower written notice of the progress of the wrongful practice exposed within a reasonable amount of time.

1.2.5 Unless the Whistleblower expressly requests otherwise, or the relevant External Reporting Channel of the respective authority reasonably believes that acknowledging receipt of the disclosure would jeopardise the protection of the Whistleblower's identity, all authorities listed below are required to promptly, and in any case within seven (7) days of receipt of the external disclosure, acknowledge that receipt.

1.2.6 The authority will make sure to carefully follow up on the report and will give the Whistleblower feedback within a fair amount of time, not to exceed three (3) months, or six (6) months in circumstances that are properly warranted. The relevant authority will inform the Whistleblower of the results of the investigation sparked by the report after making its assessment.

1.2.7 When a report is received by staff members other than those in charge of handling reports, competent authorities will make sure that these staff members are prohibited from disclosing any information that could identify the Whistleblower or the person in question. Instead, they will make sure that the report is promptly forwarded, unchanged, to the staff members in charge of handling reports, protecting the Whistleblower's anonymity (if applicable) and the confidentiality of the reported matter.

1.3 Under Maltese Law, the competent authorities for external reporting purposes are:

i. *Commissioner for Revenue:* Income tax, corporation tax, capital gains tax, stamp duties, national insurance contributions, value added tax or “revenue acts” as defined in the Commissioner for Revenue Act.

ii. *Auditor General*: Failure to observe laws, rules and regulations relating to public finance and misuse of public resources.

iii. *Commissioner for Voluntary Organizations*: Activities of a voluntary organisation.

iv. *Malta Financial Services Authority (MFSA):* The business of credit and financial institutions, the business of insurance and the activities of insurance intermediaries, the provision of investment services and collective investment schemes, pensions and retirement funds, regulated markets, central securities depositories, the carrying out of trustee business either in a professional or a personal capacity and such other areas of activity or services as may be placed from time to time under the supervisory and regulatory competence of the MFSA.

v. *Ombudsman:* Conduct involving substantial risk to public health or safety or the environment that would, if proved, constitute a criminal offence; and all matters which constitute improper practices and which are not designated to be reported to any other authority.

vi. *Financial Intelligence Analysis Unit:* Money laundering or financing of terrorism in terms of the Prevention of Money Laundering Act.

vii. *Permanent Commission Against Corruption:* Corrupt practices.

2. PROTECTION MEASURES

2.1 Qualification for Protection

2.3.1 When the following criteria are met, disclosures made by the Whistleblower constitute Protected Disclosures under the Act:

i. At the time of disclosure, the Whistleblower had a good cause to believe that the information about breaches was accurate and that it fell under the purview of this WB Policy; and

ii. The Whistleblower disclosed in line with the aforementioned procedures, either internally or externally, or made a public disclosure (i.e., made information about breaches available in the public domain).

2.1.2 If an employee deliberately divulges information that he or she knows to be false or should reasonably know to be false, the disclosure will not be regarded as a Protected Disclosure.

2.1.3 By virtue of the nature of their disclosure, anonymous whistleblowers are not entitled to the same protections as ordinary whistleblowers. However, the Whistleblower will be granted the same rights of protection as soon as (and if) their name is revealed.