

AIXCRYPTO HOLDINGS, INC.

WHISTLEBLOWER POLICY AND PROCEDURES

I. Applicability

The following Whistleblower Policy and Procedures apply to all employees, directors, independent contractors and consultants of AIXCRYPTO HOLDINGS, INC. (the “Company”).

II. Purpose

The Company is committed to conducting business in accordance with the highest ethical standards and complying with all applicable securities laws and regulations, accounting standards, accounting controls and audit practices. In that regard, the Company is establishing procedures (these “Procedures”), which have been reviewed and approved by the Audit Committee of the Board of Directors of the Company, to ensure compliance with such standards and laws. In particular, the Procedures relate to (i) the receipt, retention and treatment of complaints received by the Company regarding accounting, internal accounting controls or auditing matters or possible violations of the federal securities laws, and (ii) the confidential, anonymous submission by employees of the Company of concerns regarding questionable accounting or auditing matters, as that term is used in these Procedures, or possible violations of the federal securities laws. The Company and the Audit Committee also want to ensure that any employee wishing to submit a report of the type contemplated in these Procedures shall be free to do so without fear of dismissal or retaliation.

As used in these Procedures, the term “questionable accounting or auditing matters” includes, without limitation, (i) fraud or deliberate error in the preparation, evaluation, review or audit of any financial statement of the Company, (ii) fraud or deliberate error in the recording and maintaining of financial records of the Company, (iii) deficiencies in or noncompliance with the Company’s internal accounting controls, (iv) misrepresentation or false statements to or by a senior officer or accountant regarding a matter contained in the Company’s financial records, financial reports or audit reports or (v) deviation from full and fair reporting of the Company’s financial condition.

Given the nature of the Company’s operations in the digital asset and cryptocurrency space, “questionable matters” also include, without limitation: (i) misrepresentation of digital asset valuations or token holdings; (ii) unauthorized access to the Company’s cryptocurrency wallets or smart contracts; (iii) violations of applicable cryptocurrency regulations or digital asset licensing requirements; and (iv) market manipulation in connection with the Company’s digital assets.

III. Procedures

1. General; Filing Reports. Any person may submit a good faith report of suspected questionable accounting or auditing matters or possible violations of the federal securities laws related to the

Company. Any such allegations may be based on first-hand, direct information, or on other information from any source that the reporting person reasonably believes to be credible. As described herein, any person wishing to make such a report may choose (i) the form of the report, (ii) the designated person to whom such report may be submitted and (iii) the manner in which the report may be submitted:

A. Form of Report. A report of the type contemplated by these Procedures may be submitted orally or in writing, and may be submitted in person, by courier, or electronically (by telephone, voicemail or email) or by any other means reasonably likely to result in direct delivery of such report to a person designated under these Procedures to receive such a report.

B. To Whom Submitted.

(i) A report may be submitted to the Company's (a) ethics hotline, (b) Audit Committee (or its designee) or (c) Legal Department, whose contact information is set forth on Exhibit A. Contact information for the Audit Committee is also set forth on Exhibit A. The Company's ethics hotline can be accessed 24 hours a day, 7 days a week. The third-party ethics hotline provider will route all reports received directly to Legal Department, who shall in turn provide such reports directly to the Audit Committee.

(ii) These Procedures are designed to complement normal communication channels between supervisors and employees. Employees are encouraged to continue to raise appropriate matters with their supervisors at any time. As an alternative, employees may submit information relating to misconduct in accordance with these Procedures.

(iii) Any person who receives a report under these Procedures that appears not to have been submitted directly to the Audit Committee shall promptly make the report or a summary of the report prepared in accordance with these Procedures available to Head of Legal or the Audit Committee.

2. Confidentiality of Submission. A report may be submitted by any of the means described above (i) in the name of the party submitting the report without any limitation, (ii) in the name of the party submitting the report with a request for confidential treatment or (iii) anonymously. A request for confidential treatment means that the name of the party submitting the report will be revealed only to the person to whom the report has been submitted, to the members of the Audit Committee and to such other persons as the party receiving the report and the Audit Committee reasonably determine is advisable in order to carry out an appropriate and adequate evaluation or investigation of the matters described in the report. If a report is made anonymously, it would be a violation of these Procedures and any other applicable Company policy for the protection of whistleblowers for any employee to seek to determine the identity of the party making the anonymous submission or, upon learning through any means the identity of the party making the anonymous submission, to divulge such information to any other party. Parties are cautioned that transmission of information by way of regular email systems typically reveals the identification of the sender, and that email services provided by the Company may be reviewed by Company personnel periodically to ensure compliance with the Company's Acceptable Use Policy. As a result, submitting a report of the type contemplated by these Procedures by way of the Company's (or any other) regular email system may not be an effective means for submitting either a confidential or an anonymous report. The Company has

established, as part of its ongoing compliance program, a confidential ethics hotline referenced in Exhibit A through which persons may submit a report anonymously. In considering the manner of submitting any report under these Procedures, employees should also take into account the matters described under the heading “Handling of Reports – Notification of Others” under III.3(F) of these Procedures.

3. Handling of Reports. The following steps shall be taken with respect to each report received:

- A. Preservation.** Any person designated under these Procedures to receive a report and who receives a report in any written form (including by email) will take appropriate steps to ensure that a paper or electronic copy of the report is preserved, as the case may be. Any person designated to receive a report who receives a report by voicemail shall take appropriate steps to cause an accurate transcription to be made and to ensure that a paper copy of the transcription is preserved. Any person designated to receive a report who receives an oral report shall promptly prepare a reasonable summary of the report and shall take appropriate steps to ensure that a paper copy of the summary is preserved.
- B. Response to Reporting Party.** Upon receipt of a report, the party to whom the report has been submitted will, unless the report has been submitted anonymously, promptly acknowledge receipt of the report from the sender in writing.
- C. Audit Committee Review.** Upon receipt of a report of the type contemplated by these Procedures, the Audit Committee (or its designee) will be responsible for overseeing and directing the evaluation of the report. Such evaluation may be made independently of Company management if the Audit Committee so chooses under the circumstances. Any review and evaluation of a report will include consideration of whether the matters described in the report pertain to questionable accounting or auditing matters or possible violations of the federal securities laws, the merits of the report and whether further review and/or investigation is warranted. The Audit Committee (or its designee) shall have the authority to utilize the services of any Company personnel or retain (at the Company’s expense) any third-party consultants and/or advisors it deems appropriate under the circumstances to assist in its evaluation. Any decision by the Audit Committee to review or investigate any matter brought to its attention as a result of these Procedures will not in any way be, or be deemed to be, a determination by the Audit Committee or the Company that any actions or inactions that are the subject of the report have, in fact, occurred or constitute questionable accounting or auditing matters or possible violations of the federal securities laws. The Audit Committee (or its designee) will maintain a log of all reports of the type contemplated by these Procedures that are submitted and the status of any such reports, and the Audit Committee will establish and maintain regular procedures to review (no less frequently than quarterly) the status of reports received.
- D. Conduct of Investigations.** If the Audit Committee (or its designee) determines that further review or investigation of the matters raised in a report would be appropriate under the circumstances, the Audit Committee (or its designee) will promptly notify those parties the Audit Committee deems appropriate, promptly have such a review or investigation undertaken and authorize the retention (at the Company’s expense) of any third-party consultants and/or advisors it deems appropriate. At the conclusion of such review and/or investigation, the Audit Committee

will determine by majority vote what, if any, remedial action is appropriate. The Audit Committee will consult with and coordinate with the full Board of Directors as the Audit Committee deems appropriate. All officers, directors, employees and agents of the Company have an obligation to cooperate and comply with any review or investigation initiated by the Audit Committee pursuant to these Procedures.

- E. Delegation.** The Audit Committee may delegate the responsibility to oversee, evaluate and investigate reports to one of its members or to any other designee, such as Head of Legal, as it deems appropriate. Such designee will provide a status update of reports received at Audit Committee meetings (no less frequently than quarterly). The Audit Committee or its authorized designees shall have full authority to use Company resources to conduct any review or investigation initiated by the Audit Committee pursuant to these Procedures.
- F. Notification of Others.** At any time during a review and/or investigation of a report, the Audit Committee (or the Audit Committee's designated investigator, as applicable) or Head of Legal may notify the Company's Chief Executive Officer, Chief Financial Officer, directors or outside auditors of the receipt of a report and/or the progress or results of any review and/or investigation of the report and will provide such level of detail as may be necessary to allow for appropriate consideration by such parties of the Company's ongoing disclosure obligations, including with regard to any required officer certifications. The Audit Committee or Head of Legal may also disclose the misconduct described in a report to the Securities and Exchange Commission (the "SEC") or other governmental authority as it deems appropriate.

4. Non-Retaliation.

- A.** Neither the Company nor any officer, director, employee, contractor, subcontractor or agent of the Company will discharge, demote, suspend, threaten, harass or in any manner discriminate against any employee, independent contractor, or consultant with regard to his, her or their employment or engagement with the Company (i) based upon any lawful action of that person of the type contemplated by these Procedures, Section 806 or Section 1107 of the Sarbanes-Oxley Act of 2002 or Section 922(a) or Section 748 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, (ii) because the person has provided information to, or assisted in an investigation by (A) supervisory personnel of the Company, (B) any federal regulatory or law enforcement agency or (C) any member or committee of the Congress, regarding the activities the person reasonably believes are a violation of federal fraud laws or any rule or regulation of the SEC, or (iii) because the person filed, testified, participated in or otherwise assisted in a proceeding that has been filed or is about to be filed relating to alleged fraudulent activities or violations of SEC rules and regulations. The Company further hereby prohibits its officers, directors, employees, contractors, subcontractors and agents from taking any such retaliatory action. For the Company to implement this policy effectively, it is critical that all employees, independent contractors, consultants and other persons respond to and report any concerns of retaliatory behavior. If any such person believes that he, she or they has been subject to retaliation because of any of the actions referenced above, or is aware that any such retaliation may have been made against any other covered person, such person should report such conduct to Head of Legal or a member of the Audit Committee.

- B.** The Company will review promptly any complaint of retaliatory or other similar behavior. Complaints and investigations will be handled in a confidential manner, consistent with any corrective action that needs to be taken by the Company. Employees and other covered persons should note that they personally may be subject to criminal liability if they retaliate against a person because such person provided truthful information to law enforcement officials regarding the commission or possible commission of a federal offense.
- C. State Law Protections.** In addition to the federal protections described above, the Company is committed to complying with all applicable state whistleblower protection laws. Without limiting the foregoing, employees and other covered persons located in California are protected under California Labor Code Section 1102.5, which prohibits retaliation against any person who discloses information to a government or law enforcement agency, to a person with authority over the employee, or to another employee who has authority to investigate or correct the violation, where the person has reasonable cause to believe that the information discloses a violation of a state or federal statute, rule, or regulation. The Company will not retaliate against any person for exercising rights protected under applicable state law, and any person who believes they have been subject to such retaliation should report such concern immediately to Head of Legal or a member of the Audit Committee.
- 5. Destruction of Documents and Other Items.** Employees should be mindful of the Company's document retention policy and retain documents or other items that relate to any investigation or other official proceeding that is pending with a government department or agency. If an employee receives a request concerning the alteration, concealment or destruction of a document that the employee believes is improper, the employee is entitled to and should contact his, her or their supervisor if appropriate or any of the other persons who are designated to receive reports under these Procedures.
- 6. Digital Asset and Cryptocurrency Specific Provisions.** Given the nature of the Company's business operations in the digital asset and cryptocurrency space, the following additional provisions apply in addition to all other provisions set forth in these Procedures:
- A. Smart Contract and Wallet Security.** Any employee who becomes aware of, or has reasonable grounds to suspect, any of the following must report such concern immediately to Head of Legal, and must not attempt to investigate, remediate or disclose such matter independently: (i) a vulnerability, bug, exploit or backdoor in any smart contract deployed or used by the Company; (ii) unauthorized access to, or attempted intrusion into, any Company-controlled cryptocurrency wallet, private key, seed phrase, or multi-signature signing authority; (iii) the actual or suspected theft, misappropriation or unauthorized transfer of any digital asset held by or on behalf of the Company; (iv) the disabling, bypass or circumvention of any wallet security control, hardware security module or key management procedure; (v) any insider threat or unauthorized employee access to Company wallet credentials or custody infrastructure; or (vi) any ransomware attack, phishing scheme or social engineering attempt targeting the Company's digital asset infrastructure. All reports of this nature will be treated as urgent and will be escalated to the Audit Committee and, where required by applicable law, to relevant regulatory authorities without delay.

- B. Token and Digital Asset Transactions.** Employees who have reason to believe that any of the following has occurred or is being contemplated must report such concern promptly in accordance with these Procedures: (i) the unauthorized issuance, transfer, burn or creation of any token, coin, non-fungible token (NFT) or other digital asset in the name of or associated with the Company; (ii) the misrepresentation, concealment or inaccurate recording of any digital asset holdings, valuations or transactions in the Company’s financial records or public disclosures, including for purposes of financial reporting under applicable SEC rules and regulations; (iii) the manipulation of token prices, trading volumes or liquidity pools in a manner that could constitute market manipulation or fraud under applicable securities laws; (iv) undisclosed related-party transactions involving the Company’s digital assets, including arrangements with affiliated wallets, exchanges or decentralized finance (DeFi) protocols; (v) the use of Company digital assets for personal gain without proper authorization; or (vi) any failure to properly disclose material digital asset transactions in the Company’s SEC filings, earnings releases or other public communications, which should be reported directly to Head of Legal.
- C. Regulatory and Licensing Compliance.** Employees who become aware of potential violations of applicable cryptocurrency laws, regulations or licensing requirements must report such concerns in accordance with these Procedures. Such reportable matters include, without limitation: (i) the offering, sale or exchange of digital assets in a manner that may constitute an unregistered securities offering under the Securities Act of 1933 or the Securities Exchange Act of 1934; (ii) violations of the Bank Secrecy Act, the Financial Crimes Enforcement Network (FinCEN) regulations, or applicable state money transmission laws in connection with the Company’s digital asset operations; (iii) failure to maintain, renew or comply with required cryptocurrency exchange licenses, money services business registrations or digital asset custody licenses in any applicable jurisdiction; (iv) non-compliance with applicable sanctions laws and regulations administered by the Office of Foreign Assets Control (OFAC), including transactions with sanctioned individuals, entities or jurisdictions involving digital assets; (v) failure to file required Suspicious Activity Reports (SARs) or Currency Transaction Reports (CTRs) in connection with digital asset transactions; and (vi) any regulatory inquiry, examination, subpoena or enforcement action received by the Company relating to its digital asset activities that has not been promptly disclosed to Head of Legal. Reports involving regulatory matters will be coordinated by Head of Legal and escalated to the Audit Committee as appropriate.

IV. Questions

Employees are strongly encouraged to raise concerns they may have regarding any suspected violations of the standards contained in these Procedures. If you have a question about any aspect of these Procedures, you may submit it directly or through an intermediary to Head of Legal. All such inquiries will be treated confidentially.

EXHIBIT A — CONTACT INFORMATION

Name	Contact
Legal Department	legal@aixcrypto.ai
Audit Committee	auditcommittee@aixcrypto.ai
Ethics Hotline	ethics@aixcrypto.ai