



Etana Custody Fraud Prevention Policy

November 10, 2022

Background:

The corporate anti-fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against Etana Custody (Etana). It is the intent of Etana to promote consistent organizational behavior by providing guidelines and as signing responsibility for the development of controls and the conduct of Investigations. The Board of Directors and Management wish to make it clear that Etana has zero tolerance for the commission or concealment of fraudulent or illegal acts.

Scope of policy:

This policy applies to any fraud or suspected fraud involving employees, as well as shareholders, consultants, vendors, contractors, and outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with Etana.

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

Policy:

Management is responsible for the detection and prevention of fraud, misappropriations, and other inappropriate conducts. *Fraud* is defined as the intentional, false representation, or concealment of a material fact for the purpose of inducing another to act upon it to their injury. Each member of the management team will be familiar with the types of improprieties that might occur within their area of responsibility and be alert for any indication of fraud. Any fraud that is detected or suspected must be reported immediately according to the Reporting Suspected Fraud section below.

Actions constituting fraud:

The terms *defalcation*, *misappropriation*, and *other fiscal wrongdoings* refer to, but are not limited to, the following:

- Any dishonest or fraudulent act
- Misappropriation of funds, securities, supplies, or other assets
- Impropriety in the handling or reporting of money or financial transactions
- Profiteering as a result of insider knowledge of company activities
- Disclosing confidential and proprietary information to outside parties
- Disclosing to other persons securities activities engaged in or contemplated by the company
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company (Exception: Gifts less than \$50 in value)
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment
- Any similar or related fraud



Investigation:

The Compliance Department has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. Retaliation and retribution will not be tolerated against any employee who reports suspected fraudulent activities.

Any employee who suspects dishonest or fraudulent activity *should not* attempt to personally conduct investigations or interviews related to any suspected fraudulent act.

Members of the Investigation Unit will have:

- Free and unrestricted access to all Company records and premises, whether owned or rented
- 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

Confidentiality:

The Compliance Department treats all information received confidentially. Any employee who suspects dishonest or fraudulent activity will notify the Compliance Department. Investigation results *will not be disclosed or discussed* with anyone other than those who have a legitimate need to know.

Reporting procedures:

An employee who discovers or suspects fraudulent activity will *contact the* Compliance Department *immediately*. All reports of suspected or known fraudulent activity will be taken seriously and will be reviewed by the Compliance Department. If the investigation substantiates that fraudulent activities have occurred or was attempted, the Compliance Department will issue reports to appropriate designated personnel and, if appropriate, to Etana within 14 days.

The following unusual fraudulent thresholds must be reported to the Etana for review:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating \$5,000 or more when a suspect can be identified.
- Criminal violations aggregating \$25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating \$5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
 - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
 - Is designed to evade the BSA or its implementing regulations.
 - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.



A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

Whistleblower Protection:

Employees of Etana may not retaliate against a whistleblower for reporting an activity which that person believes to be fraudulent or dishonest with the intent or effect of adversely affecting the terms or conditions of employment (including, but not limited to, threats of physical harm, dismissal, transfer to an undesirable job assignment, demotion, suspension, or impact on salary or wages). A whistleblower is defined as an employee who informs a manager, supervisor, or Chief Compliance Officer about an activity which that person believes to be fraudulent or dishonest. Whistleblowers who believe that they have been retaliated against may file a written complaint with the Chief Compliance Officer. Any complaint of retaliation will be promptly investigated by the Chief Compliance Officer and appropriate remedial measures will be taken if allegations of retaliation are proven. This protection from retaliation is not intended to prohibit managers or supervisors from taking action, including disciplinary action, in the usual scope of their duties and based on valid performance-related factors.

Training:

Fraud awareness training shall be provided on a consistent basis to all employees.

Administration:

The Chief Compliance Officer is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed annually and revised as needed.