Anti-Money Laundering

POLICY

1. Purpose

CONVERGE ICT SOLUTIONS INC. (CICT) has zero tolerance with regards to financial crimes or to any action that violates the laws relating to Anti-Money Laundering and Terrorism Financing, including but not limited to:

- **Republic Act No. 9160:** Anti-Money Laundering Act of 2001 - An act defining the crime of money laundering, providing penalties therefore and for other purposes
- **Republic Act No. 10168:** Terrorism Financing Prevention and Suppression Act of 2012 - An act defining the crime of financing of terrorism, providing penalties therefore and for other purposes
- **Public Law 99-570:** The Money Laundering Control Act of 1986 - A United States Act that made money laundering a federal crime
- **The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)** – A United States Act that broadly affects United States federal terrorism laws and seeks to prevent money laundering and financing of terrorism among other things
- **The USA Patriot Act** – A United States Act which establishes the governmental powers for terrorism prevention and authorizes the U.S. State Department to designate terrorist organizations under the Terrorist Exclusion List

This policy aims to confirm CICT's commitment in protecting our company and employees from being used by criminals to "launder" the profits of crime. It is also to ensure that all transactions are compliant to all applicable laws relating to money laundering and at the same time sets out the guidelines and mechanisms to help CICT employees in detecting, preventing and mitigating acts and/or transactions which could involve potentially illegally obtained resources, and reporting such red flags in order to promote compliance with relevant Anti-Money Laundering Laws and avoid possible damage to the reputation, integrity, and/or stability of CICT and its employees.

This policy should be read along with CICT's Code of Business Ethics, Anti-Bribery/Anti-Corruption Policy and any other applicable policies and procedures.

2. Scope

This policy applies to the entire CICT community – from the directors, executives, officers and employees, including those of CICT subsidiaries, affiliates and third parties over which CICT has control, including joint ventures, as well as all agents, consultants, business partners and third-party representatives when they act on behalf of CICT.

3. Policy Statements

3.1. Preliminary Information

Money laundering is the process of concealing or disguising the source and nature of money or other property connected to a criminal activity (ex. terrorism, bribery, drug trafficking, or corruption) and integrating the money or properties earned or derived therefrom or related thereto into the stream of commerce, making them appear legitimate by "laundering" them through legitimate businesses or hiding their true source or owner. Through this process, the proceeds of the crimes and its perpetrator becomes difficult to be identified. Relatedly, terrorism may be financed with legitimate funds and they are sometimes called as "reverse money laundering". This happens when a legitimate business is used to fund a criminal activity.

The process for money laundering is usually completed in three stages that may contain several transactions. Any of these stages or transactions may involve CICT or its employees.

A. PLACEMENT: Placing of funds into the economy is the first stage. Material funds obtained from illegal activities are physically disposed into the market. This is normally done through creation of "phantom" companies, deposits in different financial institutions and purchase of goods among others.

B. LAYERING: Creating several complex layers of financial transactions in order to separate illicit funds from their sources, is the second stage. This is designed to cover the audit trail and provide some secrecy or anonymity. Usually, this stage depends on the activities executed during the first stage. For example, after making a huge deposit in a bank account during the first stage, the launderer will make several small transfers to different accounts to move the deposited amount and make the original deposit incomprehensible to follow. Both placement and layering are usually done using a third party.

C. REINTEGRATION: The third stage involves the attempt to make the illicit funds look entirely legitimate. If the second stage has succeeded, integration arrangements are set to place the laundered funds back into the economy in a way that they would appear to the financial system as legitimate. For example, illicit funds may be used to buy a third party business, which carefully follows regulations, and the profits are then transferred back to the criminal enterprise in such a way that appears legitimate.

These stages may occur as different phases and may overlap over a period of time. It will also depend on the money laundering mechanisms available and the requirements of the criminal organization or individual on how these stages will be used. As there is tighter enforcement of related laws in the financial sector in recent years, criminals are now employing more diverse strategies in order to proceed with money laundering without getting caught.

Following are some examples of activities that could be considered money laundering:

1. Engaging in transactions knowing that the same is facilitating a criminal activity or knowing that the funds being used are derived from proceeds of a crime.
2. Concealing the source of criminally sourced funds by subsequent transfers to disguise its origin;
3. Facilitating a transaction, willfully or recklessly disregarding the source of an investor's assets or the nature of the investor's transactions or business operations.

4.2. Consequences of Non-Compliance

Violations of any applicable laws relating to anti-money laundering and terrorism financing or this policy may result to imposition of civil sanctions, criminal prosecution and potential harm to CICT's reputation. U.S. prosecutors which also includes U.S. Department of Justice have the authority to impose penalties against CICT and in some cases, against individual employees or business partners if any individual (even a non-U.S. person) aids or causes a U.S. person to violate any of the U.S. laws indicated in this policy.

Under no circumstance shall CICT or any member of the CICT community ever participate or facilitate any money laundering activity. In addition, any breach of this policy may result to disciplinary actions, other corrective actions or even termination of employment depending on the severity of the breach. Equally, CICT will fully support any CICT employee or Third Party who declines to be involved in activities that would place the company's ethical principles and reputation at risk.

4.3. Report or Escalation of Red Flags

There will be circumstances, activities, or events that, due to their nature and the context under which they transpired, may be considered as red flags as it could be a sign of money laundering or terrorist financing activity. Although they may not be actual money laundering or terrorist financing, they can be signs of other illegal activities such as attempted fraud which also generates illicit funds.

The CICT community must be alert to any suspicious behavior or red flags when doing business with anyone. In case a red flag has been identified that could possibly violate applicable laws or this policy, he/she must do the following:

- Immediately escalate the observed red flag to the management, Human Resources, the CICT Ethics Committee, or to the CICT Legal team through its email at compliance@convergeict.com. Even if unsure if the identified activity is indeed illegal, he/she must still raise the concern for further investigation.
- In cases where the identified red flag is part of an approval process or of a transaction, the approval process or transaction must be temporarily put on hold and must be escalated to the attention of the management, Human Resources, the CICT Ethics Committee, or to the CICT Legal team.as soon as possible.
- Avoid "tipping off" or notifying the party involved as this could hinder the investigation process.

Investigations may require a thorough review of the business relationship of the affected entity to ensure that all transactions are consistent with this policy and to all applicable laws.

CICT strictly prohibits retaliation against any individual who reports in good faith actual or suspected non-compliance to any applicable laws mentioned in this policy. Such retaliation would be a ground for disciplinary actions which may include dismissal from employment.

CICT will, to the extent reasonably possible, keep confidential the identity of anyone reporting a possible violation in good faith. No one shall be demoted, suspended, terminated, harassed or even discriminated solely because he/she reported a possible violation in good faith. While individuals cannot protect themselves from discipline by reporting their own violations, self-reporting, may, in suitable situations, be considered as a qualifying factor in any disciplinary action.

4.4. Roles and Responsibilities

The Compliance Office and the CICT Legal Team shall oversee the compliance with this policy, and to all applicable laws. He/she shall be responsible for the following:

- Implementation of this policy
- Monitor any changes in the laws and be updated to any dominant techniques or cases related to Anti-Money Laundering to ensure effectiveness of this policy
- Supervision and ensure compliance within the entire CICT community
- Conduct relevant trainings within the company that is consistent with this policy
- Ensure periodic audit of CICT's compliance with this policy at least every three (3) years

4.5. Know our Customers, Suppliers and Service Providers

The Compliance Office and the CICT Legal Team shall conduct due diligence checks on customers, suppliers, service providers and such other third parties with which CICT plans to do business with. The due diligence shall be conducted with a risk-based approach, taking into consideration the appropriate factors including, but not limited to the products or services provided by Third Parties, the jurisdiction where the Third Party operates, and whether the Third Party is a publicly traded or a private company among others.

The following steps can be taken with a risk-based approach:

- Verify the identity of the Third Party.
- Confirm Third Party details. Check if the address or physical location and phone number are all valid and existing. This can be done by visiting the Third Party's business location and confirm that Third Party is operating in an ordinary manner and the business being conducted appears to agree with what is known about the Third Party or call the phone number to authenticate the given number.

- Inspect the Third Party's legal status by checking official and/or authenticated documents, such as, but not limited to tax registrations, copies of business licenses, bank references, articles of incorporation, credit agency reports or any other counterparts deemed reasonable.
- Collect information such as place/s of operations, identity and nationality of shareholders, directors, executives, administrators, as well as its regulations.
- Obtain any other information that is collected as part of ordinary business practice such as credit agency reports, financial statements, bank references, bank account information, ownership and control structure.
- Screen the Third Party against relevant anti-money laundering and sanction lists, including but not limited to the watchlist published by the Bangko Sentral ng Pilipinas, U.S. State Department's Terrorist Exclusion List, Specially Designated Nationals and Block Persons List published by the US Office of Foreign Assets Control and watchlist published by the United Nations Security Council.
- Identify the Third Part's ultimate beneficiaries and verifying them against official documentation.
- Verify that any person purporting to act on behalf of the Third Party is so authorized and identify and verify the identity and authorization of that person.

All Third Parties must be informed that it is their obligation to comply with all applicable laws relating to anti-money laundering and terrorism financing prevention laws. Once Due Diligence is collected from Third Parties, the compliance officer shall determine whether CICT could proceed dealing or transacting with the Third Party.

Records of Due Diligence shall be maintained during the lifetime of the business relationship. On a risk basis, these records must be updated annually and whenever an employee or officer detects a red flag.

4.6. Risk Assessment

The Compliance Officer, with the assistance of the legal department, shall conduct an assessment that is to be updated annually. The results of the risk assessment will be the basis for any needed improvements to this Policy.

4.7. Trainings

Anti-Money Laundering training must be provided during new hire orientation for new hires and a periodic refresher training must be conducted annually to all CICT employees with specific emphasis on employees who need to work with Third Parties.

The Compliance Officer, with the assistance of the legal department, shall maintain a list of those CICT employees who attended the trainings and shall maintain a copy of the materials used during trainings.

4.8. Internal Review and Audit

The Compliance Officer shall check CICT's compliance with this policy at least once a year by executing a formal internal review. The review will include a written report which will be given to the Board of Directors. Any insufficiencies detected during the course of the review will be accompanied by written plans on how to address identified insufficiencies in a way that is consistent with the company's policies.

The internal review will include the following:

- Updates on the laws, techniques or sample cases related to Anti-Money Laundering and economic sanctions
- Summary of the annual risk assessment
- Trainings conducted
- Any investigation executed and the reasons behind moving forward with a transaction or deciding to stop it
- Results of the internal review audit and the measures to address any identified issues or insufficiencies

4.9. Record Keeping and Data Retention

CICT shall maintain and record all relevant information gathered as part of the following:

- Due Diligence checks as well as documents relating to Third Parties' transactions with the company for a period of five (5) years after the business relationship ends in order to comply with legal obligations.
- Anti-Money Laundering trainings issued by the company to CICT employees and Third Parties, for a period of at least five (5) years after the date of training.
- Internal reviews or audits relevant to Third Parties, for a period of at least five (5) years after the date of the review or audit.

4. Related document references

- Code of Business Ethics
- Anti-Bribery/Anti-Corruption Policy

5. Annex

Sample List of Anti-Money Laundering Red Flags for Third Parties / MSAs

- Unwilling to provide identification documents or needed information is incomplete, wrong or misleading
- Difficulty in providing data requested as part of Due Diligence
- Use of fake or non-existent address

- Provides inconsistent information or expired identification
- Operations has significantly changed over time in volume or amount
- Unreasonably questions the documentation requirements and handling of information
- Refuses to provide information regarding its subsidiaries and affiliates
- Shows unusual discretion concerns, mostly regarding to its identity and type of business
- Financial information reflects asset concentration in subsidiaries or affiliates where there is an absence of audited financial statements
- Unable to identify or refuses to specify a legitimate source of funds
- Has multiple accounts under the same name for no apparent reason or purpose
- Lacks concerns about commissions, discounts, taxes, fees, risks or any other additional costs
- Transacts with public figures such as public officials
- Has a negative background such as having civil penalties of any kind, investigations relating to tax fraud, criminal activities, money laundering related activities and/or organized crimes
- Makes payments through the accounts of different individuals or entities rather than through its own account/s
- Frequently changes its payment instructions
- Seeks to bribe, threaten or even persuade CICT employees to refrain them from reporting of non-compliances relating to this policy or any applicable laws
- Frequently engages in transactions where payments are equal to the maximum amount allowed for withdrawal at financial institutions
- Requests unreasonable/questionable high or low prices
- Provides false invoices or invoices with various additional charges
- Makes an unusually large amount of overpayment and requests for a refund to be sent to an unknown Third Party
- Representative is not familiar with the basic facts about his/her company which raises the suspicion as to whether he/she is actually employed or not
- Requests to issue an invoice that does not accurately reflect an invoiced price or other material terms
- Has a broker, attorney or other agent just to facilitate the transactions which is quite unusual for this type of business