AML AND CTF COMPLIANCE QUESTIONNAIRE

NAME OF ICRE

Date Accomplished

A. BOARD OF DIRECTOR AND SENIOR MANAGEMENT OVERSIGHT

1. Board Of Director (BOD) And Senior Management (SM) Oversight

a. Is there a clear guidance from the BOD of the entity's strategic and operational plans and objectives in ensuring that the entity shall not be used as a ML and TF conduit? If so, please describe including the budget allocations to implement these plans and objectives. Have these plans and objectives been cascaded to Senior Management and responsible officers and employees? If so, state how this was done.

b. In relation to question no. 1, please describe the control policies and mechanisms (e.g. reportorial requirements, rewards and disciplinary system, training program, etc.) adopted by the BOD to attain these policies and objectives.

c. Please describe the entity's framework for ML and TF prevention. What are the roles of the BOD, Senior Management, Compliance Office, Internal Audit and other Offices in ML and TF prevention? What reports are required to be submitted to the BOD to assist them in their decision-making processes?

d. Please describe the risk management system relative to ML and TF prevention.

e. Does the Compliance Office/Officer report directly to the BOD? If not, to whom does the Compliance office/officer report? How frequent is this done?
f. Please describe the authorities delegated by the BOD to the Compliance Office and the AML and CTF Compliance Officer related to ML and TF prevention.

g. What other relevant oversight does the BOD and Senior Management exercise to ensure attainment of the entity's plans and objectives relative to ML and TF prevention?

2. Identification, Measurement, Monitoring And Controlling Of Risks And Problems Related To ML And TF

a. Have you conducted risk profiling of all existing customers? If not all, what percentage of the total customers count had been profiled?

b. Have you conducted an assessment of the risks and vulnerabilities that your entity is exposed into? Please describe how the assessment was done.

c. What identified risks and vulnerabilities is the entity exposed into and how are these risks and vulnerabilities measured, monitored and controlled by the BOD and/or SM?

3. Self Assessment Systems That Are Either Pro-Active, Through Compliance-Testing, Or Reactive, Through Internal Audit

a. Have you conducted an over-all assessment of the entity's level of compliance with the Anti-Money Laundering Act of 2001 (AMLA), under Republic Act (R.A.) No. 9160, as amended by R.A. Nos. 9194, 10167, 10365 and 10927, the Terrorism Financing Prevention and Suppression Act (TFPSA), under R.A. No. 10168, their respective Implementing Rules and Regulations (IRR), Circular Letter (CL) No. 2018-48, as amended and other relevant laws, IC and AMLC issuances? Please describe how this was done and state the frequency of the assessment.

b. Based on the assessment, please state in percentage the level of compliance of the entity.

c. How are deviation from pre-set guidelines as well as deficiencies and weaknesses noted during internal and external audits corrected and what are the mechanisms undertaken to monitor implementation of corrective measures?

d. Has your entity recently undergone an internal audit on AML and CTF Compliance? If yes, please summarize the key findings and/or
recommendations that were noted in the most recent internal audit report and set out the measures that the BOD has undertaken to address these findings and to monitor the same.

<table>
<thead>
<tr>
<th>KEY FINDINGS</th>
<th>RECOMMENDED ACTIONS</th>
<th>PROGRESS/DEVELOPMENT</th>
</tr>
</thead>
</table>

e. Has your entity recently undertaken compliance testing of other departments, units, offices and branches that is independent of the internal audit? If yes, please describe the process (whether on-site inspections were conducted) and summarize the key findings and/or recommendations that were noted in the most recent compliance testing report and set out the measures that the BOD has undertaken to address these findings and to monitor the same.

<table>
<thead>
<tr>
<th>KEY FINDINGS</th>
<th>RECOMMENDED ACTIONS</th>
<th>PROGRESS/DEVELOPMENT</th>
</tr>
</thead>
</table>

4. Management Information System

a. Has the entity carried out an assessment of the effectiveness of the management information system as well as the AML and CTF electronic or manual, as applicable, monitoring system? Please specify how this is done.

b. What reports are being submitted to the BOD or Board level/approved Committee to assist them in their decision making processes relative to ML and TF prevention, who signs them and how frequent are they being required?

c. Does the entity keep annual statistics on red flags systems alerts, ML investigations, CT reports, ST reports broken down as to the nature? If so, which Office requires and maintains the same? Please provide copies of the statistics.

d. Does the entity keep track dispositions of red flag systems alerts? If so, which Office requires and maintains the same? Please provide copies of the tracking report.

5. Capability Of Compliance Office In Managing The Entity’s MTPP
a. Provide the names and contacts details of AML and CTF Compliance and Alternate Compliance officers. Also, provide the name of another officer designated by the company who is responsible and accountable for all record keeping requirements under the AMLA, as amended, TFP SA, their respective IRR, CL No. 2018-48, as amended and other relevant laws, IC and AMLC issuances.

b. Describe the structure of the Compliance Office including the financial, human and technical resources, delegated authorities, reporting and communication line, duties and responsibilities of the Office as a whole and of individual officers and staff together with their qualifications and experience as well as standards in hiring new employees, and control mechanisms (such as the power to monitor and ensure compliance including the authority to impose sanctions or give incentives or rewards when necessary) of the Office in ensuring that the pre-set objectives are adhered by responsible officers and employees in the different Departments, Groups, Units and/or Branches?

c. How are newly adopted policies and procedures as well as subsequent changes thereto assessed (as adequate or inadequate) and how are the results of the assessment communicated to the BOD, to Senior Management, to different Departments, Units, Groups, Sub-groups and to the Branches up to the frontliners and/or agents?

d. How is the adequacy of AML and CTF training assessed? Please specify in detail.

e. Have you taken the necessary measures to prevent criminals or their associates from holding or being the beneficial owners of a significant or controlling interest or holding a management function, including membership in the Board or any Committee within your entity? If yes, please describe the measures taken.

f. Do you have a screening process that ensures high standards when hiring employees? If yes, please indicate the specific policy provisions applicable.

g. Are the directors and senior management subject to internal "fit and proper" requirements including a check on their expertise and integrity? If yes, please provide the relevant policy provisions. If election, selection or appointment is based on family ties, please indicate.

h. Do you ensure that your foreign branches and subsidiaries observe AML and CTF measures consistent with the Philippine's legal requirements? If yes, please indicate the specific policy provisions.
i. In connection with the last question, was there an instance when the home country supervisor where a foreign branch or subsidiary is located has prohibited the branch or subsidiary from observing the Philippine laws, rules and regulations because it is prohibited by local (i.e. host country) laws, regulations or other measures? If yes, have you notified the Insurance Commission (IC) of this directive? Please indicate the specific legal provision(s) that provide(s) the legal basis for this requirement.

j. How are the provisions of the Money Laundering And Terrorist Financing Prevention Program (MTPP) disseminated to responsible officers, employees and agents and how are their compliance assessed and monitored?

k. What other relevant management practices does the Compliance Office exercise to manage its MTPP and ensure attainment of the entity's plans and objectives relative to ML and TF prevention?

6. Nature Of Weaknesses Noted And Ability To Address Existing And Potential Risks And Problems

a. Has your entity undergone a previous AML and CTF Compliance Checking by the IC? If yes, please summarize the key findings and/or recommendations that were noted in the most recent AML and CTF report and set out the measures that the BOD has undertaken to address the findings and to monitor the same.

<table>
<thead>
<tr>
<th>KEY FINDINGS</th>
<th>RECOMMENDED ACTIONS</th>
<th>PROGRESS/DEVELOPMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

b. How are deviation from pre-set guidelines as well as deficiencies and weaknesses noted during internal and external audits corrected and what are the mechanisms undertaken to monitor implementation of corrective measures?

7. Institutional Risk Assessment

a. Has your entity undergone an Institutional Risk Assessment? If yes, when was this conducted?

b. Has your entity documented the risk assessment and findings? If yes, please summarize the key findings and/or recommendations that
were noted in the most recent Institutional Risk Assessment and set out the measures undertaken to address the findings and to monitor the same.

<table>
<thead>
<tr>
<th>KEY FINDINGS</th>
<th>RECOMMENDED ACTIONS</th>
<th>PROGRESS/DEVELOPMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

c. Has your entity considered all the relevant risk factors, including the results of national and sectoral risk assessment, before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied? If yes, please provide a summary.

B. MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM

1. Customer Identification, Verification and Ongoing Monitoring Process

a. Does the entity apply a risk-based approach to combating money laundering and terrorist financing? If so, please provide an overview of these policies and procedures. The overview should (1) portray the entity's philosophy towards risk-based (does it form an integral part of the entity's business framework?), (2) indicate how the relevant risk assessments are undertaken and their bases to help determine the policy and its practical application, and (3) describe the mechanism by which permitted variations from the generally applicable standards are promulgated, and what arrangements, if any, are in place to monitor the continuing suitability of the exceptions. Please provide the basis in the entity's MTPP.

b. Does your entity permit the opening of anonymous accounts, accounts in fictitious names and other accounts not otherwise under the true and full name of the customer/client? If yes, please indicate the approximate number of accounts, pertinent policies and procedures for opening and the level of approving authority.

c. Does your entity undertake customer due diligence (CDD) measures when:

   i. Establishing business relations?
ii. Carrying out transactions with non-clients?
iii. Carrying out occasional transactions?
iv. Dealing with trustee, nominee, agent, or intermediary, applying CDD not only on the latter but also on the trustors or principals?
v. Dealing with juridical entities that have no business substance in their own right but through which transactions may be conducted, applying CDD on the entities' beneficial owner?
vi. The entity has doubts about the veracity of previously obtained customer identification document or data?

For each of the above, please describe in detail the CDD process and the specific provision in the MTPP that apply.

d. Does your entity undertake customer due diligence (CDD) measures on the beneficiary(ies) of life insurance and other investment related insurance policies? Please describe in detail the CDD process and the specific provision in the MTPP that apply.

e. Explain the CDD requirements applicable to potential individual customers stating the minimum information to be obtained, IDs acceptable and its classification based on reliability, if any, and policy in updating identification information citing the specific internal policy provisions.

f. Explain the CDD requirements applicable to potential customers that are juridical entities and the persons acting on their behalf such as but not limited to the President and the authorized signatory/ies stating the minimum information to be obtained, IDs acceptable and its classification based on reliability, if any, measures to prevent the unlawful use of legal persons in relation to money laundering and terrorist financing and policy in updating identification information citing the specific internal policy provisions.

g. Does your entity identify the beneficial owner of juridical entities dealing with your entity and verify the information acquired? If yes, please describe in detail including the specific internal policy provisions.

h. Does your entity verify the true identity of customers, including validating the truthfulness of the information and confirming the authenticity of the identification documents presented, submitted and provided by the customer, using reliable and independent sources, documents, data, or information? If yes, please describe in detail including the specific internal policy provisions.
i. Does your entity verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person? If yes, please describe in detail including the specific internal policy provisions.

j. Does your entity identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from reliable sources, such that the entity is satisfied that it knows who the beneficial owner is? If yes, please describe in detail including the specific internal policy provisions.

k. Does your entity understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or the business relationship with its customers? If yes, please describe in detail including the specific internal policy provisions.

l. Does your entity, on the basis of materiality and risk, conduct ongoing due diligence on the business relationship of existing customers? If yes, please describe the extent/scope of this obligation and indicate the specific internal policy provisions.

m. Does your entity perform enhanced due diligence for higher risk categories of customer, business relationship or transaction and does it apply to existing customers? If yes, please explain including reference to the list of customers considered as high-risk, criteria and factors considered in applying EDD, types of measures required, control mechanisms for managing the risks associated with dealing with these customers, validation procedures and the specific internal policy provisions. Also, provide number of high-risk customers per category.

n. Does your entity apply reduced due diligence where there is low risk of ML or TF? If yes, please explain providing details of any applicable conditions/standards and specific internal policy provisions. Is this permitted with regard to customers that are resident in another country? If yes, please explain further.

o. What does your entity do in cases where it is unable to satisfactorily complete the CDD measures required by existing internal rules or under CL 2018-48, as amended, the AMLA, as amended, and its IRR? Please indicate the specific internal policy provisions that apply.

p. What are your obligations with regard to establishing business
relationships with a politically exposed person, his/her immediate family relative, his/her close relationship/associates, entities related to them? Please describe the existing policies governing these arrangements, including the standard of due diligence that apply to them on account opening, control mechanisms to address the risks associated with dealing with them, and updating of identification information with references to specific internal policy provisions.

q. Does your entity allow non-face-to-face transactions (transactions with trustee, nominee, agent or intermediary accounts including account opening)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

m. Do any of your businesses make use of third parties, referral by brokers, intermediaries, fiduciaries, affiliates, subsidiaries and the like (Collectively called as third parties)? If Yes, please identify the third-parties and the due diligence undertaken on the third parties. Please also identify the business areas which make use of third parties, the approval process for introducing customers/clients, the type of relationship, and whether or not such third parties perform the CDD process that would usually be undertaken by the entity;

n. Do you rely on third parties to perform some of the elements of the CDD process (face-to-face or gathering of the minimum information)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

o. Are there instances where you outsource some of the elements of the CDD process (face-to-face or gathering of the minimum information)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

p. What are your obligations with regard to business relationships and transactions with persons (including legal persons and other financial institutions) who are nationals or citizens of foreign jurisdiction or geographical location which do not or insufficiently apply internationally accepted AML and CTF standards, as determined by relevant domestic or international bodies? Please provide the internal policy provisions, which serve as basis for these obligations.
q. Are there measures in place to ensure that your entity is advised of concerns about weaknesses in the AML/CTF systems of other countries? If yes, please describe these measures and how these concerns are incorporated into the entity’s Program.

r. Are there measures in place to ensure that funds collected by or transferred through non-profit organizations are not diverted to support the activities of terrorists or terrorist organizations? If so, please specify what these measures are and indicate the specific policy provisions.

s. What are your obligations with regard to relevant United Nations Security Council Resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing? Please provide the internal policy provisions, which serve as basis for these obligations.

2. Record Keeping And Retention Process

a. Please describe the record-keeping obligation including the type of records and information that should be maintained. Please indicate the specific internal policy provisions.

b. Do you maintain all necessary records on transactions, both domestic and international and, if so, for how long following completion of the transaction? Who are the designated custodians that shall be accountable and responsible for safekeeping these documents?

c. Do you maintain records of the identification information and documents and data, account files and business correspondence and, if so, for how long following the termination of an account or business relationship?

d. Do you ensure that all customer and transaction records and information are available on a timely basis to competent authorities? If yes, please indicate the designated custodian that shall be accountable and responsible for safekeeping and making these records available with references to specific internal policy provisions.

3. Covered And Suspicious Transaction Reporting
a. Do you have an electronic money laundering transaction monitoring system in place? If yes, is it internally developed or purchased from a vendor, and does it have the following automated functionalities?

i. Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;

ii. Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;

iii. Investigation – checks for given names throughout the history of payment stored in the system;

iv. Can generate all the CTRs of the ICREs accurately and completely with all the mandatory field properly filled up;

v. Must provide a complete audit trail;

vi. Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and

vii. Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of senior management whether or not a report was filed with the AMLC.

b. If no, please describe how you manually perform the functionalities mentioned above.

c. Do you pay special attention to unusual transactions? If yes, how do you define unusual transactions? And what type of special measures do you implement in managing them? Please indicate the specific internal policy provisions for this requirement.

d. Are you required to report to the AMLC a suspicious transaction report (STR), when you suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity? Please describe the scope of the obligation, the decision process and the decision maker within the entity (whether or not to file an STR) with references to the specific internal policy provisions that mandate reporting.

e. Does the obligation to make an STR also apply when you suspect or have reasonable grounds to suspect that funds are related to terrorism? If yes please describe the scope of this obligation, the decision process and the decision maker within the entity (whether or not to file an STR) with reference to the specific internal policy provisions that mandate reporting.

f. Other than the 6 specified circumstances for filing an STR, what other instances do you report an STR or an alert has been tagged using the
last item- any transaction that is similar or analogous to any of the foregoing, i.e. tax evasion, malversation of public funds, bribery, etc?

g. What is the legal protection against potential liability available to your officers and/or staff who report their suspicion in accordance with the legal obligation to report? Please describe, by reference to the specific internal policy provisions, the scope of the protection in terms of who would benefit from it and the types of liability against which it is available.

h. Do you prohibit your officers and staff from disclosing ("tipping off") to any person the fact that an STR, CTR or related information is being reported or provided to the AMLC? If they are, please describe the scope of this prohibition by reference to the specific internal policy provisions.

4. Employment And Training Program

a. Please indicate the standards that apply when hiring new staff to the Compliance Office, the Internal Audit and the entity as a whole?

b. Please describe the entity's AML training and refresher program with specific references to the level of training and focus on the participant, the Office tasked to implement the program, the financial, human and technical support that that Office has been given and frequency of offering.

c. Are the staffs of the Compliance Office and Internal Audit Office provided with training for combating money laundering and terrorist financing that is different from the staff of other offices? Please give details.

d. Do you have an on-going employee training on AML and CTF? if yes, please indicate the last employee training on AML and CTF and the schedule for the year as well as the specific policy provisions for this requirement.

C. INTERNAL CONTROLS AND AUDIT

1. What is the structure of the Internal Audit Office including the financial, human and technical resources, delegated authorities, reporting and communication line, duties and responsibilities of the Office as a whole and of individual officers and staff together with their qualification and experiences as well as standards in hiring new staff, and control
mechanisms of the Office in ensuring that the pre-set objectives are adhered by responsible officers and staff in the different Department, Groups, Units and/or Branches?

2. Do you establish and maintain internal procedures, policies and controls to prevent ML and TF? How do you communicate these to the officer, staff and employees? Please provide details with reference to the applicable policy provisions.

3. Do you maintain an adequately resourced and independent audit function that tests compliance with these procedures, policies and controls? If yes, please indicate the available resources, financial, human, and technical and the specific policy provisions for this requirement.

D. IMPLEMENTATION

1. Covered And Suspicious Transaction Reporting Policies And Procedures

a. Do you have an electronic money laundering transaction monitoring system in place? If yes, is it internally developed or purchased from a vendor, and does it have the following automated functionalities?

i. Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;

ii. Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;

iii. Investigation – checks for given names throughout the history of payment stored in the system;

iv. Can generate all the CTRs of the ICREs accurately and completely with all the mandatory field properly filled up;

v. Must provide a complete audit trail;

vi. Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and

vii. Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of senior management whether or not a report was filed with the AMLC.

b. If no, please describe how you manually perform the functionalities
mentioned above.

c. Do you pay special attention to unusual transactions? What type of special measures do you implement in managing them?

d. Are you required to report to the AMLC a suspicious transaction report (STR) when you suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity? Please describe the scope of the obligation, the decision process and the decision maker within the entity (whether or not to file an STR).

e. Does the obligation to make an STR also apply when you suspect or have reasonable grounds to suspect that funds are related to terrorism? If yes please describe the scope of this obligation, the decision process and the decision maker within the entity.

f. Other than the 6 specified circumstances for filing an STR, what other instances do you report an STR or an alert has been tagged using the last item- any transaction that is similar or analogous to any of the foregoing, i.e. tax evasion, malversation of public funds, bribery, etc?

g. What is the legal protection against potential liability available to your officers and/or staff who report their suspicion in accordance with the legal obligation to report?

h. Does the Compliance Office keep annual statistics on red flags systems alerts, ML investigations, CT reports, ST reports broken down as to the nature? Please provide copies of the statistics.

i. Does the Compliance Office keep track dispositions of red flag systems alerts? Please provide copies of the tracking report.

j. Do you prohibit your officers and staff from disclosing (“tipping off”) to any person the fact that an STR, CTR or related information is being reported or provided to the AMLC?

2. **Risk Based And Tiered Customer Acceptance, Identification, Verification And Ongoing Monitoring Policies And Procedures**

a. Does your entity undertake customer due diligence (CDD) measures when:
   i. establishing business relations?
   ii. carrying out transactions with non-clients?
   iii. carrying out occasional transactions?
   iv. dealing with trustee, nominee, agent, or intermediary, applying CDD not only on the latter but also on the trustors or principals?
   v. dealing with juridical entities that have no business substance in their own right but through which financial transactions may be
conducted, applying CDD on the entities' beneficial owner?

vi. the entity has doubts about the veracity of previously obtained customer identification document or data?

b. Does your entity undertake customer due diligence (CDD) measures on the beneficiary(ies) of life insurance and other investment related insurance policies?

c. Does your entity identify the beneficial owner of juridical entities dealing with the entity and verify the information acquired?

d. Does your entity verify the true identity of customers, including validating the truthfulness of the information and confirming the authenticity of the identification documents presented, submitted and provided by the customer, using reliable and independent sources, documents, data, or information?

e. Does your entity verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person?

f. Does your entity identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable sources, such that the entity is satisfied that it knows who the beneficial owner is?

g. Does your entity understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or the business relationship with its customers?

h. Does your entity, on the basis of materiality and risk, conduct ongoing due diligence on the business relationship of existing customers?

i. Does your entity perform enhanced due diligence for higher risk categories of customer, business relationship or transaction and does it apply to existing customers?

j. Does your entity apply reduced due diligence where there is low risk of ML or TF? What does your entity do in cases where it is unable to complete the CDD measures required by existing internal rules or under CL 2018-48, as amended, the AMLA, as amended, and its IRR?

k. What does your entity do in cases where it is unable to complete the CDD measures required by existing internal rules or under the CL 2018-48, as amended, the AMLA, as amended, and its IRR?

l. In case of non-face-to-face services, does the entity ensure that control measures to address risks associated with this type of business relationships or transactions are implemented?
3. **Record-Keeping And Retention Policies And Procedures**

   a. What are the type of records and information that your entity maintains?

   b. Do you maintain all necessary records on transactions and, if so, for how long following completion of the transaction? Who is/are the designated custodian that shall be accountable and responsible for safekeeping these documents?

   c. Do you maintain records of the identification documents and information, account files and business correspondence and, if so, for how long following the termination of an account or business relationship?

   d. Do you ensure that all customer and transaction records and information are available on a timely basis to competent authorities? If yes, please indicate the designated custodian that shall be accountable and responsible for safekeeping and making these records available.

   e. Do you conduct compliance testing to ensure that all units and/or branches maintain and safely store KYC and transaction records?

   f. Does the Internal Audit cover an assessment of compliance of the record-keeping and retention process?

4. **Continuing Education And Training Program**

   a. Are newly hired employees required to attend AML and CTF training?

   b. Is there an existing training and refresher program for all responsible directors, officers and staff? Please provide a copy of the program.

   c. Are the staffs of the Compliance Office and Internal Audit Office provided with training for combating money laundering and terrorist financing that is different from the staff of other offices?

   d. Do you have an on-going director and employee training on ML and TF prevention? If yes, please indicate the last training and the schedule for the year.

   e. Do you conduct a regular post-test on directors and employees to
gauge their understanding of AMLA, as amended, its IRR, CL 2018-48, as amended, and other IC and AMLC relevant regulations?

f. Provide statistics on education and training provided to responsible directors, officers and employees covering the immediately preceding year.

<table>
<thead>
<tr>
<th>Classification (e.g. new employees; regular employees; board of directors; agents; officers; etc.)</th>
<th>Total Number Per Classification</th>
<th>Number of Training Hours</th>
<th>Date of Training</th>
<th>Number of directors, officers and employees who completed the training</th>
</tr>
</thead>
</table>

E. ICRE DATA/ INFORMATION

1. Provide information on the total asset of the entity as of 31 December of the immediately preceding year.

2. Provide a list of all products being offered/sold according to classification by the ICRE.

3. Provide data/ information on products covering the immediately preceding year.

<table>
<thead>
<tr>
<th>Product Classification</th>
<th>Total Premium/ Contract Price/ Membership Fees Received</th>
<th>Number of Issued or Sold Policies/ Pre-Need Plans/ HMO Agreements</th>
<th>Number Outstanding Policies/ Pre-Need Plans/ HMO Agreements</th>
<th>Number of Policies/ Pre-Need Plans/ HMO Agreements Surrendered/ Cancelled/ Lapsed</th>
</tr>
</thead>
</table>

4. Provide number of suspicious and covered transactions reported to AMLC covering the immediately preceding year.

<table>
<thead>
<tr>
<th>Type of Report</th>
<th>Number of Reports Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Transaction Reports</td>
<td></td>
</tr>
<tr>
<td>Covered Transaction Reports</td>
<td></td>
</tr>
</tbody>
</table>
CERTIFICATION

The undersigned President and AML and CTF Compliance Officer of the company certify that the responses and explanations set forth in the above AML and CTF Compliance Questionnaire are true, complete and correct of our own personal knowledge and/or based on authentic records.

Signed in the City of ______________ on the ______ of _______ 20__.

___________________________
PRESEDENT
Signature over printed name

___________________________
AML AND CTF COMPLIANCE OFFICER
Signature over printed name

SUBSCRIBED AND SWORN to before me this ______day of ________________, 20____, by the following who are all personally known to me (or whom I have identified through competent evidence of identity) and who exhibited to me their respective identification document as follows:

<table>
<thead>
<tr>
<th>NAME</th>
<th>ID NO.</th>
<th>DATE/ PLACE ISSUED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTARY PUBLIC

Doc. No. ______;
Page No. ______;
Book No. ______;
Series of 20____.