Anti Money Laundering Policy

Advanced Technologies and Services, Inc.

Table of Contents

1. Introduction

Advanced Technologies and Services, Inc ("ATS" or the "Company"), confirm their commitment to the values and ethical principles of the Company, and to combat that certain activity known as "Money Laundering"[1] and the Financing of Terrorism through this Policy.

In this sense, ATS is really interested in preventing attempts, through any of the companies, to conceal or disguise the illegal origin of resources derived from criminal activities, or to help Third Parties evade the legal consequences of their actions.

The Anti-Money Laundering and Combating the Financing of Terrorism legal framework (hereinafter referred to as "AML-FT") is based on a series of international agreements and recommendations, such as the "40 Recommendations of the Financial Action Task Force"[2], which have been adapted to the regulation of each country to apply these prevention standards.

ATS has developed an Integrity and Compliance Program which includes, among other things, its Code of Ethics and this Policy. Any violation of our Code of Ethics, our internal policies or applicable laws, rules and regulations, may lead to civil and criminal penalties ranging from fines and imprisonment to the forfeiture of goods being imposed on individuals and the Company.

2. Purpose

This policy was prepared to set the principles and guidelines applicable in this matter and have an appropriate and efficient control, surveillance and audit system, so that the Company can ensure that all activities conducted by the Company or on its behalf are subject to our Code of Ethics, this Policy and applicable laws, rules and regulations.

This is how we reasonably ensure that ATS or any related companies are not used to channel resources of illegal origin or intended to promote or finance terrorism.

Through this policy, you will become aware of the principles and procedures the Company must have in place and that you, as an Employee and/or Third Party, must observe to protect ourselves, the Company, its shareholders and any Third Parties from possible violations to applicable laws, rules and regulations.

[1] Depending on the country, the "Money Laundering" phenomenon may also be called "Asset Laundering", "Legitimization of Capitals", "Legitimization of Illegally Obtained Proceeds", "Cleaning Assets", "Laundering of Goods or "Cleaning Capitals / Assets". However, for purposes of easy reading in this document, the term "Money Laundering" will be used with the same meaning of all the aforementioned terms.

[2] The Financial Action Task Force (FATF, or GAFI, for its Spanish acronym) is the international organization that has designed strategies or "best international practices" to prevent Money Laundering and the Financing of Terrorism".

3. Scope

This Policy is applicable and mandatory to you and all our Employees and Third Parties, in every country where we operate; therefore, it is important to know, understand and put into practice the principles and values contained herein.

4. Definitions

Risk-Based Analysis: Systematic use of available information and materials to determine the probability that a possible fact, act or risk may happen, as well as the magnitude or impact of their possible consequences, based on the vulnerabilities identified under those circumstances.

Authority (Authorities): Government entities of each country with powers in the Prevention or Prosecution of Money Laundering and Terrorist Financing.

VB: Vulnerable Businesses, also known as "Designated Non-Financial Businesses and Professions", or DNFBPs, a classification mentioned in FATF recommendations[3]. This refers to business sectors that domestic laws consider at higher risk of being used for Money Laundering.

Notices or Reports: A communication that, based on a legal provision, the Company must submit before an Authority, or before the Compliance Officer under this Policy.

Actual/ Final Beneficiary: This means the individual that ultimately has or controls the proceeds of profits and executive decisions regarding a Customer and/or the individual on whose behalf the transaction is completed. This term also includes the people who effectively have final control over a person or agreement.

Customer or User: An individual or entity who executes documents or completes transactions with the Company with the purpose of buying a product or service offered or traded by the Company.

Contract: Agreement between two or more persons to create, transfer, modify or terminate rights and obligations.

Due Diligence: Review of the background of an entity or an individual, either before or after commercial relationships are established and/or a Contract is signed, in order to identify potential legal, financial, operational, reputational or contagion risks.

Report of Irregularities: A complaint filed in good faith and with reasonable motives, to report confidentially and without retaliation, possible breaches within ATS or any of its Subsidiaries.

https://sanctionscanner.com/knowledge-base/designated-non-financial-businesses-and-professions-dnfbp-205

Diagnostic Assessment: This is a document used to determine if any of the Company business activities is subject to a special regime under applicable Anti-Money Laundering and Counter-Terrorist Financing laws. If applicable, it specifies the level of compliance and, in general, includes a risk assessment and rating for the risk of the Company being used for Money/ Asset Laundering or Terrorist Financing.

Employee(s): Any person or persons hired under an individual or collective bargaining agreement by ATS or any of its Subsidiaries.

Concealment: Behavior that hinders or makes it difficult to discover a criminal or illegal activity.

Risk Assessment: This means the process of identification and analysis of risks relevant to the Company achieving its purposes, to prevent them, or to determine an appropriate response in the event the risk materializes.

Financing of Terrorism: Transfer of resources or provision of services to be used for terrorist acts.

FATF: Financial Action Task Force.

Money Laundering: i) The conversion or transfer of goods with the purpose of concealing or disguising their illegal origin or helping any person involved in a crime to evade the legal consequences of his/her acts; ii) concealing or disguising the actual nature, origin, location, arrangement, movement or property of goods or the legitimate right to such goods.

Compliance Officer: This is the department of ATS responsible for establishing an Integrity and Compliance Program with appropriate and efficient policies and control, surveillance and audit systems, and in charge of constantly monitoring compliance with integrity standards across the organization. compliance@atso.com

Subsidiary's Compliance Officer: This means the department in the Subsidiary responsible for implementing, disseminating and overseeing observance of the Integrity and Compliance Program, according to the criteria, indications and assessments of the Compliance Officer of ATS.

Policy: This means the statement of general principles that the Company agrees to comply with; therefore, it is of general application to Employees, executives, directors and shareholders.

Whistleblower Portal: The internal platform provided by ATS for Employees or Third Parties to report anonymously and confidentially any conduct that infringes upon the Company's Code of Ethics and/or policies is under development.

Procedure: A document that defines specifically how to carry out a process or an activity, describing all the process from beginning to end.

Integrity and Compliance Program: This program was developed and is overseen by the Compliance Officer, and includes, without limitation: (i) preparing Company policies and other guidelines to comply with laws, rules and regulations in effect; (ii) the identification, prevention and mitigation of operational and legal risks in order to ensure the long-term reputational value of the Company and create more certainty around its value chain; (iii) the implementation of appropriate and efficient control, monitoring and audit systems allowing the ongoing and periodic verification of compliance with integrity standards throughout the organization; and (iv) managing

operations of the Whistleblower Portal and coordinate training in compliance.

Risk: This means the likelihood of a negative event happening and of its negative effects or impact, the existence of which represents a threat (source of danger) to the Company and makes it vulnerable to their effects.

Subsidiary: Any entity controlled by ATS.

Third Party (Parties): Distributors, representatives, advisors, commercial partners, agents, brokers, customers, contractors, managers, lobbyists, consultants or suppliers who are part of the value chain of ATS or represent the Company in interactions with another Third Party, a Government or Civil Servants. This includes civil society organizations and education, charitable, cultural or sports institutions the Company is considering for a Donation.

5. General Guidelines

"Money Laundering" is a crime that consists of hiding the illegal origin of goods and resources obtained through illegal activities; this criminal action damages the economy, companies, and ultimately, people like us.

This criminal phenomenon funds, and encourages and promotes, crimes such as corruption, fraud, tax evasion, forgery, smuggling, piracy, and other very serious crimes that affect personal security, such as drug trafficking, kidnapping, weapon trafficking and many more. Therefore, fighting "Money Laundering" stops the economic cycle that allows the development of criminal activities, weakens organized crime and strengthens the economy in general.

As to "Terrorist Financing", it is also a crime that involves obtaining goods or support for people or organizations in order to carry out operational or logistical actions or activities with the purpose of causing fear or terror among a population.

Due to these reasons, at the international level, countries have been asked to pass laws encouraging companies to create methodologies and controls for the "Prevention" of "Money Laundering and Terrorist Financing" crimes. In order to make specific laws more efficient, very severe legal sanctions have been imposed, ranging from several years of imprisonment for individuals committing crimes, to criminal liability for companies, as well as fines and seizures.

Accordingly, it is fundamental for ATS and its Subsidiaries to adopt an Anti-Money Laundering and Combating the Financing of Terrorism Policy, with a methodology based on operations effectively performed and a Risk-Based Analysis that may allow them to identify possible vulnerabilities to Money Laundering and Terrorist Financing and so, implement appropriate actions to control and mitigate Risks.

In this sense, and to ensure compliance of Company standards, its Code of Ethics and laws in effect in each of the jurisdictions where it operates, ATS has issued this Anti Money Laundering and Combating the Financing of Terrorism Policy, based on the following minimum prevention measures:

- Risk-Based Analysis;
- Procedures Manual;

· Determination of Internal Prevention Structures;
· Training and Dissemination Programs; and
· Prohibition of Activities leading to Money Laundering.

5.1. Risk-Based Analysis

The Company must efficiently design and implement a Risk-Based Analysis focused on Money Laundering or Financing of Terrorism, designed to identify activities actually performed and match them to the level of risk that it is exposed to, derived from the products, services, customers, countries, countries, geographic areas, distribution channels or technologies in its operations. The respective analysis must include at least the following documents:

5.1.2. Diagnostic Assessment

The Company should have a Diagnostic Assessment prepared by the Compliance Officer and the Compliance Officer of the Subsidiary to identify the activities that it effectively performs and be able to determine its level of vulnerability in terms of Anti-Money Laundering and Financing of Terrorism.

The result of this procedure must be a document called “AML-FT Diagnostic Assessment”.

This is a document used to determine if any of the Company business activities is subject to a special regime under applicable local Anti-Money Laundering and Counter-Terrorist Financing [6]laws.

5.1.3. Risk Matrix

The Company will have an Anti-Money Laundering and Combating Financing of Terrorism Risk Matrix, prepared jointly by the Compliance Officer and the Compliance Office of a Subsidiary, and called “AML-TF Risk Matrix”.

This matrix will be designed to provide an overview of the Risks that affect the Company, the likelihood and impact of these events, the mitigation actions planned, the assessment of their effectiveness and, if applicable, the determination and follow-up of mitigation action improvements for a better Risk management control.

5.2. Procedure Manual

In order to prevent and detect acts, omissions or operations that may favor, help or cooperate for Money Laundering and/or the Financing of Terrorism, the Subsidiaries will prepare an operations manual containing the criteria, measures and internal procedures necessary for such purpose. Such manual must be approved and authorized by the Compliance Officer and it shall include, at least, the following policies and procedures:

5.2.1. Identify and Know your Third Parties

Depending on the level of vulnerability determined in the AML-FT Diagnostic Assessment, applicable laws and the special regime to which it is subject by law, if any, the Company must have and efficiently implement a Policy and a documented Procedure to identify Third Parties and prepare their transactional profile, as well as any consequences in the event of default.

These documents will establish requirements to fully and efficiently identify Third Parties interacting with the Company, and to monitor them as necessary to detect unusual activities that should be reported, and the final Beneficiary of the commercial relationship, if any.

Likewise, to ensure that the Company is not used for Money Laundering and Financing of Terrorism operations, proper procedures will be established to conduct the due diligence of its supplies and commercial partners

[6] This refers to activities that may be identified as vulnerable by the specific local law, such as financial and FATF Designated Non-Financial Businesses and Professions.

in order to detect any business or operation contrary to the law and, if applicable, terminate the commercial relationship.

The level of detail, both of the Policy and of the Procedure, will be determined by the rating of the Company business, the applicable local law, the special regime it is subject to, if any, and the Diagnostic Assessment authorized by the Compliance Officer.

5.2.2. Preparation and Maintenance of Files and Records

Depending on the degree of vulnerability determined in the AML-FT Diagnostic Assessment, applicable laws and the special regime that the Company is subject to by law, if any, the Company will preserve, protect, safeguard and prevent the destruction or concealment of the information and supporting documentation of specific operations, as well as information that identifies its Customers, Users, suppliers and commercial partners.

For purposes of the preceding paragraph, the Company will have and efficiently implement a Policy and a documented procedure to specify:

- The obligation to generate and effectively and efficiently complete identification files for Third Parties (distributors, representatives, consultants, commercial partners, agents, intermediaries, customers, contractors, managers, lobbyists, consultants or suppliers);
- The information, data or documents that files must contain;
- How often will information contained in the files be updated;
- The way in which information must be gathered for the files;
- The methodology to preserve, classify, and as applicable, safeguard confidential information efficiently and effectively;
- The methodology to guarantee the integrity, availability, auditability and confidentiality of the information;
- The people responsible for collecting and safeguarding the files;
- The period that the files must be kept;
- The methodology for accessing files; and
- The methodology for the exchange of internal information, coordinating the exchange of information between the Subsidiaries, as well as their internal areas, and the supply of information about customers and relevant activities, in order to identify, oversee and investigate irregular or suspicious operations.

In addition, in the aforementioned Procedure, the Company will clearly establish the

consequences in the event of any breach of the procedures set forth.

The level of detail, both of the Policy and of the Procedure, will be determined by the rating of the Company business, the applicable local law, the special regime it is subject to, if any, and the Diagnostic Assessment authorized by the Compliance Officer.

5.2.3. Black List Screening

Depending on the level of vulnerability determined in the AML-FT Diagnostic Assessment, applicable laws and the special regime to which it is subject by law, if any, the Company must have and efficiently implement a Policy and a documented Procedure to identify black lists (domestic and international) subject to verification, the frequency of such review, and the key persons for such review, as well as any consequences in the event of default.

"Key person for review" shall mean the Customers, Users, suppliers, operational commercial partners, shareholders and main executives of the Company.

If any key person is included in any of the referred black lists, either domestic or international, the consequence will be the immediate suspension of any relationship or the completion of any act, activity, operation or service related to the person included in such lists.

The level of detail, both of the Policy and of the Procedure, will be determined by the rating of the Company business, the applicable local law, the special regime it is subject to, if any, and the Diagnostic Assessment authorized by the Compliance Officer.

5.2.4. Use of Cash Restriction

Depending on the level of vulnerability determined in the AML-FT Diagnostic Assessment, applicable laws and the special regime to which it is subject by law, if any, the Company must have and efficiently implement a Policy and a documented Procedure to set limits for the use of cash to make payments or payments in full, and to accept payments in full or payments for activities or operations with Third Parties, as well as any consequences in the event of default.

In this sense, the Company must establish in its Policies and principles the need to verify that any payment for operations or activities performed by the Company is made through legally incorporated financial institutions in their countries of origin.

The level of detail, both of the Policy and of the Procedure, will be determined by the rating of the Company business, the applicable local law, the special regime it is subject to, if any, and the Diagnostic Assessment authorized by the Compliance Officer.

5.2.5. Submission of Notices/ Internal Reports

Depending on the level of vulnerability determined in the AML-FT Diagnostic Assessment, applicable law and the applicable special regime, if any, the Company will have and efficiently implement a Policy and a documented Procedure to:

- Clearly establish and explain the types of Anti-Money Laundering and Counter

Terrorist Financing Notices/ Reports. Both internal and external;

- "Notices or External reports" means those that, due to some legal provision of a country, must be submitted to a specific Authority;
- "Notices or External reports" means those identified in the Policy and the Procedure prepared for such purpose. Irrespective of the Notices or Internal reports deemed relevant by the Company, it must ensure that at least the following are prepared:
  - 24-hour Internal Notices or Reports. Those used by the Compliance Officer of the Subsidiary to highlight an activity or operation related to a Third Party that may materialize any of the risks included in the AML-FT Risk Matrix.
  - Concerning Internal Notices or reports. Those in which the Compliance Officer of the Subsidiary highlights an activity or change of behavior or transactional profile of any member of the Company, employee, executive or shareholder.

- The methodology that should be followed to submit the corresponding Notices or Reports;
- The time periods to present them;
- The person responsible for their submission; and
- The generation of compliance statistics and their submission to the Compliance Officer.

The level of detail, both of the Policy and of the Procedure, will be determined by the rating of the Company business, the applicable local law, the special regime it is subject to, if any, and the Diagnostic Assessment authorized by the Compliance Officer.

5.3. Determination of Internal Prevention Controls

The Company must clearly establish the internal controls designed to comply with Anti Money Laundering and Combating the Financing of Terrorism obligations, in accordance with applicable specific laws, the special regime that the Company is subject to by law, if any, and the Diagnostic Assessment authorized by the Compliance Officer setting concrete obligations and their specific basis.

Irrespective of the foregoing, the Company will:

- Appoint at least the Compliance Officer of the Subsidiary, with the duty to comply with all Anti-Money Laundering and Money Laundering obligations contained in this Policy;
- Designate the Compliance Officer as the body in charge of coordinating Anti-Money Laundering and Combating the Financing of Terrorism Company Policies.

5.4. Training and Dissemination Programs

The Company, along with the Compliance Officer, must prepare and efficiently implement two programs: one for "Training" and other for "Dissemination" of Anti-Money Laundering and Combating the Financing of Terrorism matters.

5.4.1. Training Program

The Company will prepare and implement an efficient program of differentiated Training on Anti-Money Laundering and Combating the Financing of Terrorism, adapted to the people receiving the training and the respective applicable law, which must be authorized by the Compliance Officer.

In this sense, the Training Program will be designed at least for:

- Internal Personnel;
  - Top Management;
    - Internal structures; and
    - Employees in general.
  - External personnel
    - Commercial partners or third parties.

5.4.2. Dissemination Program

The Company will prepare and implement a **Dissemination** Program, directed to the general public, focused on Anti-Money Laundering and Combating the Financing of Terrorism, which must be authorized by the Compliance Officer.

In this sense, the Dissemination Program will include at least the following:

- Emphasis on the commitment of all the members of the Company to the Prevention of Money Laundering and the Financing of Terrorism;
- The existence of this Policy and the consequences of not following it;
- The existence of applicable laws and the consequences of incurring in violations;
- News that may reinforce the relevance of the topic; and
- Communication mechanisms with the Compliance Officer and the Compliance Officer of the Subsidiary.

5.5. Prohibition of Activities leading to Money Laundering

When analyzing the phenomenon of Money Laundering, the general consensus is that, although Money Laundering is an autonomous crime, it implies predicate offenses, which generate the financial flow that will later be subject to a process of "laundering".

In fact, to have a proper understanding of the threat faced by an organization of being used for Money Laundering, it is necessary to know the environment in which those previous crimes are committed and generate the illegal proceeds that will later be subject to Money Laundering, as described by GAFILAT in the document "ANALYSIS OF REGIONAL THREATS ON MONEY LAUNDERING" which states[7]:

> "45. One of the main features of the ML threats is the fact that their realization can bring benefits that may be the subject of legitimation. In this line, a number of crimes can be identified, which are committed with some relevance in the region and that enable those who carry them out to get a
>
> significant income that can be subject to ML, both within or outside the region. Let's not forget that the very concept of ML, despite its character of autonomous offense, implies the prior commission of another crime (predicate or base offense) from which an economic income is derived, which needs to be legitimized in order for it to be used.

In the same document, GAFILAT identified as threats for Money Laundering:

· Human trafficking for purposes of sexual exploitation;
· Region affected at all stages of drug trafficking;
· Existence of organized crime based on different areas of the region; · Public corruption;
· Illegal trafficking of human beings (migrants);
· Smuggling of goods and counterfeit products; and
· Tax offenses.

In this order of ideas, it is worth mentioning that ATS and its Subsidiaries are committed, as a policy, to refraining from engaging or maintaining relationships with companies linked to the aforementioned activities, particularly tax offenses.

In this sense, ATS and its Subsidiaries have pledged to prevent tax evasion, and are firmly determined to comply with their tax obligations, irrespective of the country where they are created. This commitment is specifically expressed in the following concrete activities:

- Unrestricted observance of the Code of Ethics and other policies issued by América Móvil; of Conventions and International Treaties on tax, anti-corruption and anti money laundering matters; the Fiscal Code of the United States of America; applicable financial information standard; and national and local laws applicable in each of the countries where it trades.
- Always truthfully and transparently preparing accounting books and records. · Ban on illegal operations to obtain any undue tax benefit.
- Promote business practices with companies with a good standing regarding their tax obligations, avoid commercial relationships with those about which not enough and verified information is available, and avoid connections with companies that are known or should be known for their bad reputation regarding tax obligations, national or international.
- Conduct or allow internal or external audits to verify compliance with applicable tax laws, rules and regulations.

ATS and its Subsidiaries also agree to refrain from using illegal benefits in countries classified as tax havens for purposes of fiscal planning, and from creating companies in countries considered tax havens.

If, owing to our business operations, the acquisition of a company that has subsidiaries in countries considered tax havens prior to the purchase is justified, we pledge to liquidate or sell such subsidiaries to comply with our goal of strictly complying with the tax laws of the countries where we trade.

This is verifiable because ATS develops and keeps a transparent, traceable and truthful fiscal framework, accurately and timely complying with all fiscal requirements of a privately-held-S-Corporation.

6. Policy Compliance Oversight and Verification

The Compliance and Internal Auditing Officers are responsible for supervising, overseeing and, as applicable, auditing the due compliance of all provisions in this Policy, and periodically assessing their efficacy.

The Compliance Officer is also responsible for evaluating periodically the Integrity and Compliance Program which includes, among other things, a series of measures intended to prevent acts of Corruption. It is also responsible for providing guidance to Employees regarding this Policy, via this email address compliance@atso.com, along with line managers.

If any audits are necessary, they will be conducted regularly and randomly in the various departments of the Company.

All Company Employees must support and cooperate with the work teams in charge of such audits, refraining from obstructing or blocking audit processes and from providing incorrect or false information.

Remember that we all must comply and ensure compliance with this Policy and report any act contrary to it, by messaging the compliance officer at compliance@atso.com

7. Training and Dissemination

It is extremely important for us to understand and implement all actions described herein, and with the purpose of promoting a culture of transparency, ethics and values, América Móvil offers its Employees and Third Parties online or in-person courses, which will be promoted through the Company's official means of communication, in order to provide training to help them understand the concepts, scope, and situations that may occur during daily operations, and to express any concerns they may have.

We at ATS or its Subsidiaries are responsible for attending the allocated sessions, complying with the specified times and requested assessments.

8. Cooperation and Coordination

The Compliance Officer is responsible for preparing and making its best efforts to harmonize this Policy with respect to the Subsidiaries. However, the Subsidiaries will be responsible for complying with applicable legal obligations before the Authorities of each individual country.

Therefore, Subsidiaries shall have in place an internal compliance procedure fit for the specific Anti-Money Laundering and Combating the Financing of Terrorism obligations assumed in each country, approved by the Compliance Officer, taking into account the particular risks faced and obligations imposed in each country.

Furthermore, Subsidiaries shall ensure that they have in place efficient mechanisms that may allow them to cooperate and, as applicable, coordinate internal efforts to develop and implement

Policies and activities designed to prevent Money Laundering and Terrorist Financing.

9. Sanctions

Failures to comply with this Policy may lead, both for Employees and Third Parties, to administrative, labor, or even criminal sanctions, depending on the seriousness of the particular act, which will be determined in accordance with internal workplace regulations and/or applicable laws, rules and regulations.

Within ATS, the Ethics Committee of each Subsidiary shall be the authority of last resort to determine sanctions in the event of default of this Policy, without prejudice to such defaults being also penalized by applicable laws and authorities having jurisdiction.

10. Whistleblower Portal

To file a complaint in connection with any default to this Policy or our Code of Ethics, contact the compliance officer at compliance@atso.com

Each Employee of ATS and Third Party have the right and an obligation to directly report their line manager to the Compliance Officer in connection with any behavior that infringes this Protocol or any applicable laws, rules, regulations, Policies or internal procedures and, in general, any non-ethical conduct.

Further, it is our duty to cooperate with any internal or external investigation and keep it confidential. Employees who make a false or misleading complaint may be subject to disciplinary actions.

Remember that failure to report a serious breach of ethics can have disciplinary consequences for you, since you may be concealing an unethical or criminal act. Reports can be made anonymously if the person filing the report wishes to do so; however, we encourage informants to leave some contact details for follow-up during the investigation.

It Is also important to note that nothing in this Policy is meant to discourage employees from reporting any misconduct directly to law enforcement authorities. In such cases, our suggestion is that it should be reported to Legal and/or the Compliance Officer, so that they can cooperate with the authorities, if necessary.

All reports will be investigated by ATS's Compliance Officer, who reports to the Audit and Corporate Practices Committee of ATS.

The Compliance Officer is in charge of supervising and operating the email code for reports, and will send to the Ethics Committees of each subsidiary the corresponding reports so that they can be investigated properly.

11. Questions and Comments

If you have questions, comments or suggestions regarding this Policy, please contact us in the following email address: compliance@atso.com