PEP POLICY

PayNox EOOD

ID number: 208071994

Legal address: Bulgaria, City of Burgas, 19 Marahydyk St., fl. 2, office 1

INTRODUCTION

This Politically Exposed Persons (PEP) Policy establishes the framework for identifying, assessing, and managing the risks associated with business relationships involving individuals who hold, or have held, prominent public functions. PEPs, by virtue of their positions and influence, may present a higher risk of involvement in bribery, corruption, and money laundering.

The purpose of this policy is to ensure that PayNox Ltd complies with applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) laws and regulations by implementing appropriate procedures to identify PEPs and apply enhanced due diligence measures when necessary.

This policy applies to all employees, departments, and business units of PayNox Ltd, and must be integrated into the customer onboarding, monitoring, and risk management processes.

DEFINITIONS

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a prominent public function. These individuals, due to their roles and influence, are considered higher risk in terms of exposure to bribery, corruption, or money laundering activities.

A Domestic PEP refers to someone who holds or has held a prominent public position within their own country, such as members of the national government, judiciary, central banks, or state-owned enterprises.

A Foreign PEP is someone who holds or has held a prominent public function in a foreign country. This includes officials in foreign governments or foreign public institutions.

An International Organization PEP is an individual who holds or has held a senior management position in an international organization. These roles typically include directors, deputy directors, or board members of organizations such as the United Nations, the World Bank, or the International Monetary Fund.

Family Members of a PEP include individuals who are closely related to a PEP, such as their spouse or partner, children and their spouses or partners, and parents.

Close Associates of a PEP are individuals who have close business or personal relationships with a PEP. This may include persons with joint ownership of companies or legal entities, those involved in the same business arrangements, or individuals acting on behalf of a PEP.

Enhanced Due Diligence (EDD) refers to additional procedures and controls that are applied to high-risk customers, including PEPs. This involves identifying the source of funds and wealth, obtaining approval from senior management before establishing a business relationship, and conducting ongoing monitoring of the relationship and transactions.

SCOPE

This Politically Exposed Persons (PEP) Policy applies to all departments, employees, consultants, agents, and subsidiaries of PayNox Ltd., across all jurisdictions where the company operates. It is relevant to all business units involved in onboarding, managing, and monitoring customers and their transactions.

The policy covers all client types, including individuals, corporate entities, beneficial owners, and other relevant parties who may qualify as PEPs or be associated with PEPs. It also applies to third parties acting on behalf of clients, such as intermediaries or legal representatives.

This policy is integral to the company's overall anti-money laundering (AML) and counter-terrorist financing (CTF) framework. It must be applied during the initial customer due diligence process, throughout the duration of the business relationship, and as part of ongoing monitoring and risk assessments.

LEGAL AND REGULATORY FRAMEWORK

This policy is based on and aligns with applicable local and international legal standards and regulatory expectations concerning anti-money laundering (AML) and counter-terrorist financing (CTF). The identification and management of Politically Exposed Persons (PEPs) are key elements in global efforts to prevent financial crimes.

The company adheres to the guidelines set forth by the Financial Action Task Force (FATF), which requires enhanced due diligence for PEPs as part of its Recommendations. These standards are recognized internationally and are implemented into the laws and regulations of many countries.

Additionally, the company complies with specific national regulations applicable in the jurisdictions in which it operates. These may include, but are not limited to, the European Union's AML Directives, the USA PATRIOT Act, the UK Proceeds of Crime Act, and other regional or local AML/CTF laws and supervisory guidance.

This policy ensures that the company fulfills its obligations under these frameworks by establishing appropriate internal controls, procedures, and oversight for managing risks related to PEPs.

CORE PRINCIPLES

The company is committed to upholding the highest standards of integrity, transparency, and regulatory compliance in managing the risks associated with Politically Exposed Persons (PEPs). The following core principles guide the implementation of this policy:

The company adopts a risk-based approach in identifying and managing relationships involving PEPs. This means applying proportionate measures based on the level of risk each PEP poses, taking into account their role, geographic exposure, and the nature of the relationship.

Enhanced due diligence (EDD) measures are mandatory for all PEPs. These include identifying the source of wealth and funds, obtaining senior management approval before establishing or continuing the relationship, and conducting ongoing monitoring of the account and transactions.

All employees must ensure that PEPs are identified at the earliest possible stage of the relationship, ideally during customer onboarding. Any existing clients must be reviewed regularly to determine if they have become PEPs since the initial screening.

The company utilizes reliable and up-to-date screening tools and databases to identify PEPs, as well as to detect close family members and associates.

Employees must receive regular training on identifying and managing PEPs, including how to recognize red flags and apply internal procedures effectively.

Strict confidentiality must be maintained throughout the PEP identification and monitoring process, and all findings must be properly documented and stored in accordance with recordkeeping requirements.

IDENTIFICATION OF PEPs

The identification of Politically Exposed Persons (PEPs) is a critical component of the company's customer due diligence and anti-money laundering processes. All new and existing clients must be screened to determine whether they qualify as PEPs, or are closely associated with a PEP, at the time of onboarding and throughout the business relationship.

PEP identification must occur during the initial stages of customer onboarding. Clients are required to disclose whether they or any of their beneficial owners, senior executives, or related parties are PEPs. This information must be confirmed using reliable sources, such as global PEP databases, government publications, or other trusted screening tools.

The company must also identify individuals who are family members or close associates of PEPs, as these persons may pose similar risks. Screening systems must be updated regularly to ensure continued accuracy and relevance.

If a client is identified as a PEP or becomes a PEP after the relationship has started, enhanced due diligence (EDD) procedures must be immediately applied. This includes re-evaluating the client's risk level, obtaining senior management approval, and documenting all actions taken.

Staff are required to escalate any suspected or confirmed PEP status to the compliance department for verification and further review.

ENHANCED DUE DILIGENCE (EDD)

Enhanced Due Diligence (EDD) is a more rigorous process of investigating and verifying the identity of individuals or entities considered to be high-risk in terms of financial transactions or business relationships. This in-depth process is typically used to comply with anti-money laundering (AML) and counter-terrorism financing (CFT) regulations. EDD is triggered when an individual or transaction presents a higher level of risk due to factors such as the person being a Politically Exposed Person (PEP), being from a high-risk country, or engaging in suspicious transactions.

The EDD process involves far more scrutiny than standard due diligence (CDD). When conducting EDD, organizations go beyond basic identity verification to check the source of wealth and funds of the customer or entity. This ensures that the funds involved in a transaction are legitimate and not the result of criminal activity. For example, organizations will verify the true identity of a person or entity, including obtaining detailed documentation, and check against global watchlists, sanctions lists, and PEP lists to identify any possible risks or associations with criminal behavior.

In addition to verifying identity, EDD involves background checks to assess whether the individual or entity has any criminal history or involvement in financial crimes. This could include researching public records, looking for negative media coverage, and reviewing the ownership structures of companies to identify potential links to illicit activities. If a customer or entity is deemed high-risk, institutions may request further documentation and conduct more thorough checks before proceeding with a business relationship or transaction.

Continuous monitoring is another key aspect of EDD. Once an individual or entity is flagged as high-risk, organizations must monitor their transactions and behaviors over time. This ongoing surveillance helps to detect any changes in patterns or suspicious activities, such as large or irregular transactions, that could indicate money laundering or terrorism financing. Regular re-screening of high-risk clients is essential to ensure that new risks are identified and mitigated promptly.

For transactions or clients deemed to be high-risk, approval from senior management or the compliance officer may be necessary before proceeding with any business activities. If suspicious activities are identified during EDD, organizations are required to report them to the relevant regulatory authorities, typically through Suspicious Activity Reports (SARs).

The importance of EDD lies in its ability to protect organizations from being inadvertently involved in criminal activities, mitigate financial crime risks, and ensure compliance with regulatory frameworks. By thoroughly investigating high-risk individuals and entities, businesses can better safeguard their operations and reputation, ensuring that they are not exposed to the legal, financial, or reputational damage that could arise from associations with illicit activities.

RISK ASSESSMENT

A risk-based approach to evaluating Politically Exposed Persons (PEPs) is a strategy that focuses on assessing the level of risk associated with each individual PEP based on various factors. This approach allows organizations to apply more targeted and resource-efficient measures, focusing on higher-risk PEPs while still ensuring compliance with regulatory requirements. By considering the specific circumstances of each PEP, organizations can determine the level of due diligence required and decide on appropriate actions to mitigate risks.

In this approach, organizations assess the risk posed by a PEP by evaluating several key factors. One of the primary factors is the PEP’s position and the level of influence they hold. For example, a head of state or a senior government official will generally be considered higher risk than a lower-ranking political figure. The rationale is that individuals in high-ranking positions may have greater access to state funds, influence over public resources, and opportunities for corruption, bribery, or embezzlement.

Another critical factor is the country or jurisdiction the PEP is associated with. PEPs from countries with high levels of corruption, weak governance, or ongoing political instability represent a higher risk for money laundering and financial crimes. On the other hand, PEPs from countries with strong regulatory frameworks and low corruption levels might pose less risk, although they still require monitoring.

The PEP's connections also play a role in the risk assessment. This includes evaluating the individual's family members, close associates, and business partners. Criminal activities, corrupt practices, or money laundering schemes may involve not only the PEP but also their relatives and associates. Therefore, understanding these relationships is crucial to determining the level of risk.

The nature of the business or transaction involving the PEP also impacts the risk assessment. For instance, a PEP involved in high-value transactions, particularly those across borders or involving shell companies, might indicate a higher risk. Additionally, the frequency and size of the transactions may also provide insights into the risk level associated with the individual.

An important element of the risk-based approach is the tiered level of scrutiny applied based on the findings. If a PEP is identified as high risk, the organization will conduct Enhanced Due Diligence (EDD), which includes verifying the source of wealth and funds, investigating any potential links to criminal activities, and assessing the legitimacy of transactions. For lower-risk PEPs, standard due diligence procedures might be sufficient, but continuous monitoring and periodic re-evaluation are still necessary.

Ultimately, the goal of the risk-based approach is to allocate resources effectively by focusing on PEPs who pose the greatest potential for financial crime risk, ensuring that the institution remains compliant with regulations while avoiding unnecessary costs and disruptions. This approach allows for a balanced, efficient, and dynamic system of managing and mitigating risks related to PEPs.

RECORD KEEPING

The duration for retaining PEP-related records generally depends on the legal and regulatory requirements of the jurisdiction in which a financial institution or business operates. Typically, organizations are required to retain these records for at least five years after the end of the business relationship or the completion of the transaction that prompted the Enhanced Due Diligence (EDD) or Politically Exposed Person (PEP) identification.

The five-year retention period is a common standard in many jurisdictions, including the European Union under the Fourth Anti-Money Laundering Directive and in the United States under the Bank Secrecy Act. This period allows organizations to maintain access to customer identification records, transaction details, and any enhanced due diligence findings in case of regulatory reviews, audits, or investigations. If suspicious activity reports (SARs) are filed or if a transaction is flagged for potentially illegal activity, some jurisdictions may require that records be kept for a longer period, sometimes up to seven years or more, especially if the records are part of ongoing investigations or legal proceedings.

It is important to note that regulatory requirements may vary by jurisdiction. While the Financial Action Task Force (FATF) recommends a minimum of five years, some countries may have stricter regulations that necessitate a longer retention period.

The types of records that must be kept include customer identification information, risk assessments, transaction records, and the results of any enhanced due diligence efforts.

In certain cases, especially when records are involved in ongoing investigations or litigation, institutions may need to retain them for a longer duration until the investigation or case is resolved. Retaining these records for the required period ensures that institutions are in compliance with anti-money laundering (AML) regulations, provides documentation for audits or investigations, and protects against legal or reputational risks.

STAFF RESPONSIBILITIES AND TRAINING

Employee responsibilities in PEP detection and reporting are vital to ensuring an organization remains compliant with anti-money laundering (AML) regulations and effectively manages the risks associated with Politically Exposed Persons (PEPs). Employees, particularly those in compliance, customer service, or risk management roles, are responsible for identifying potential PEPs, conducting due diligence, and reporting suspicious activities. Their responsibilities include adhering to internal policies, using appropriate tools and systems, and escalating any concerns appropriately.

Employees are first responsible for following the organization's established customer due diligence (CDD) procedures, which include identifying customers and verifying their identities. If a customer is flagged as a PEP or their background indicates potential risks associated with their political or public position, employees are responsible for ensuring that enhanced due diligence (EDD) measures are applied. This involves verifying the source of wealth and source of funds, ensuring that any wealth or transactions linked to the PEP are legitimate and not connected to illegal activities.

In addition, employees must continuously monitor transactions for any unusual or suspicious behavior. PEPs often engage in transactions that may raise red flags, such as large, frequent, or complex transfers, especially across borders. Employees are responsible for identifying these red flags and reporting them to the compliance or risk management team. This might include escalating any concerns or suspected illicit activity, particularly if the transactions appear inconsistent with the PEP's known financial profile.

Employees must also ensure that they are aware of relevant sanctions or watchlists and use screening tools or databases to check whether a customer is a PEP or is on any international or local blacklists. Many organizations have systems in place to automatically flag PEPs during onboarding or during ongoing monitoring, but employees must ensure that these tools are correctly applied and reviewed regularly.

When employees detect a PEP or suspicious activity, they are responsible for reporting it promptly to the compliance department or the designated money laundering reporting officer (MLRO). This could involve filing a Suspicious Activity Report (SAR) if suspicious activity is identified, ensuring that the report includes all necessary information for investigation. The timeliness and accuracy of these reports are crucial, as delays or inaccuracies could lead to regulatory penalties or expose the organization to greater risks.

Furthermore, employees must maintain a high level of confidentiality throughout the detection and reporting process, especially when dealing with sensitive information regarding PEPs or suspicious activities. This ensures that the integrity of investigations is maintained and that the organization complies with data protection laws.

In essence, employees are crucial in the early stages of PEP detection by identifying individuals in politically sensitive roles, performing the required due diligence, reporting suspicious activities, and contributing to the overall risk management framework of the organization. Their vigilance, adherence to protocols, and timely communication help prevent financial crimes and ensure compliance with AML regulations.

MONITORING AND REVIEW

The periodic review of PEP status is a critical component of an organization's overall anti-money laundering (AML) and counter-terrorism financing (CFT) strategy. It involves regularly re-assessing the political exposure status of clients or entities flagged as Politically Exposed Persons (PEPs) to ensure that the risk profile remains up to date and that any changes in the individual’s political or public role are identified promptly. This process helps ensure that the organization remains compliant with regulations and adequately manages risks related to PEPs.

Over time, a PEP’s status could change due to a shift in their political or public role, which may either increase or decrease their risk profile. For example, a PEP who was previously a high-ranking official in a government might retire, thus reducing their risk level. Conversely, an individual who was not initially flagged as a PEP could rise to a higher political office, triggering the need for re-evaluation.

Periodic reviews typically involve verifying whether the client is still considered a PEP or whether any changes to their status have occurred. This review might be triggered by a number of factors, such as changes in the PEP's political roles, changes in family members' or associates' statuses, or even changes in the country of residence or origin. In some cases, periodic reviews may also involve reassessing the source of wealth and source of funds, particularly if there have been significant changes in the financial behavior of the PEP, their family, or business associates.

Regular screening against updated PEP lists, sanctions lists, and other relevant watchlists is a part of the periodic review. Organizations need to monitor changes in these lists and ensure that they are applying the most current data when conducting their reviews. This process is essential to detect new risks, such as if the PEP is now associated with a high-risk jurisdiction or linked to criminal activities.

The frequency of periodic reviews can vary depending on the institution's internal policies, the risk profile of the client, and regulatory requirements. High-risk PEPs might be reviewed more frequently—sometimes quarterly or semi-annually—while lower-risk PEPs might be reviewed annually. In any case, the review should be thorough, consistent, and well-documented to demonstrate compliance with regulatory obligations.

The goal of the periodic review is to ensure that the organization remains vigilant and proactive in its efforts to detect and mitigate risks related to PEPs. By regularly updating risk profiles, financial institutions can respond to changes in a PEP's circumstances, manage evolving risks, and continue to meet their legal and regulatory obligations in preventing financial crimes.

REPORTING OBLIGATIONS

Reporting obligations in the context of Politically Exposed Persons (PEPs) primarily relate to the duty of financial institutions and other relevant entities to report any suspicious activities, transactions, or relationships involving PEPs that might be linked to money laundering, terrorism financing, or other illegal activities. These obligations are part of the broader framework of anti-money laundering (AML) and counter-terrorism financing (CFT) regulations that financial institutions must follow to prevent illicit financial activities.

One of the key obligations is to report suspicious transactions. If an organization suspects that a transaction involving a PEP may be related to criminal activities, it must file a Suspicious Activity Report (SAR) with the relevant authorities. This report should include detailed information about the transaction, the parties involved, and the reasons why the transaction is considered suspicious. For example, if a PEP’s transaction appears to be unusually large, involves unusual structures (such as shell companies), or lacks a clear legitimate purpose, it may need to be reported.

In addition to suspicious transactions, customer due diligence (CDD) and enhanced due diligence (EDD) records involving PEPs must be maintained and made available to regulatory bodies upon request. This includes keeping thorough records of the PEP’s identification details, the source of their wealth and funds, and any other relevant information obtained during the risk assessment and due diligence process.

These records should be kept for at least five years (or longer in some jurisdictions), even after the business relationship with the PEP ends.

Internal reporting procedures also play an essential role. Employees working in compliance, customer service, or risk management positions must follow internal protocols to escalate potential issues related to PEPs. When employees detect any suspicious activity or have concerns about a particular PEP, they are responsible for promptly notifying the compliance officer or money laundering reporting officer (MLRO) within the organization. This ensures that the issue is assessed by senior management and can be escalated to regulatory authorities if necessary.

Reporting obligations are typically regulated by government authorities or regulatory bodies. These agencies often provide specific guidance on when and how suspicious activity should be reported, as well as the content required in a SAR. Failure to comply with reporting obligations can result in severe penalties, including financial fines, reputational damage, and even criminal prosecution in extreme cases.

In summary, the reporting obligations related to PEPs are designed to ensure that institutions remain vigilant against financial crime. They require organizations to report suspicious activities, maintain accurate records of PEP-related due diligence, and follow internal escalation procedures to flag potential risks. By meeting these obligations, organizations help to prevent money laundering and terrorism financing while maintaining compliance with regulatory requirements.

POLICY APPROVAL AND REVISIONS

Policy approval and revisions are essential aspects of maintaining an effective and compliant framework for dealing with Politically Exposed Persons (PEPs) in an organization. These processes ensure that the organization's policies remain current, compliant with evolving regulations, and responsive to emerging risks.

The policy approval process typically starts with the drafting or review of the PEP-related policies by the relevant departments, such as compliance, legal, and risk management. This draft policy will outline the steps for identifying PEPs, conducting due diligence, monitoring, and reporting any suspicious activity, and ensuring ongoing compliance with anti-money laundering (AML) and counter-terrorism financing (CFT) regulations. The policy is then submitted for approval to the board of directors, executive management, or designated governance body within the organization. Approval ensures that senior leadership is aligned on the importance of PEP monitoring and that the policy aligns with both internal goals and external regulatory expectations.

Once approved, the policy becomes part of the organization's formal framework, and it serves as a reference for employees and stakeholders involved in customer due diligence (CDD), enhanced due diligence (EDD), and reporting processes. These policies must also be communicated clearly to relevant personnel and incorporated into training programs to ensure that everyone understands their roles and responsibilities in handling PEPs.

Revisions to the policy are necessary when there are changes in laws, regulations, or organizational operations that affect how PEPs should be handled. Regulatory changes—such as updates to anti-money laundering laws, revisions to sanctions lists, or the introduction of new financial crime risks—often prompt policy revisions. Additionally, changes within the organization, such as new business lines, expanded geographical presence, or technology updates (like improved screening tools), may necessitate adjustments to the PEP monitoring and reporting procedures.

The process of revising the policy involves several steps. First, a comprehensive review of the current policy is conducted to identify any gaps or areas for improvement. This review is often carried out by the compliance or legal team, sometimes in collaboration with external consultants or auditors, especially if there are significant regulatory changes. Once any revisions are identified, the updated policy is again submitted for approval by senior management or the board of directors, just as in the initial approval process.

Once approved, the revised policy is communicated across the organization, and updated training programs are rolled out. Employees should be informed of any changes that affect their responsibilities in identifying and managing PEPs. Ensuring that everyone is up-to-date on the latest policies and procedures is critical for maintaining compliance.

In addition to formal policy revisions, regular monitoring and testing of the policy's effectiveness is essential. This can involve internal audits, risk assessments, and the use of feedback from employees and regulators to identify any issues or inefficiencies in the policy. Ongoing revisions should be made as necessary to address these findings.

In summary, the approval and revision process for PEP-related policies ensures that an organization's practices remain in line with regulatory requirements, operational changes, and emerging risks. Regular reviews and updates, along with senior management involvement, are key to maintaining a robust framework for managing PEP risks and protecting the organization from potential legal and financial harm.