البنك الإسلامي العربي
ARAB ISLAMIC BANK

سياسة مكافحة غسل الاموال وتمويل الإرهاب

Anti Money Laundering & Counter – Terrorism financing Policy &

Know Your Customer(KYC) إجراءات قاعدة إعرف عميلك

2023

المحتويات

ضبط الاصدار

إقرار الوثيقة	
الاعداد	**الموافقة**
الاسم : دائرة التنظيم واجراءات العمل	**الاسم: مجلس الادارة**
التاريخ:	**التاريخ:**

ضبط الإصدار		
رقم الاصدار	**تاريخه**	**اسباب التعديل**
01	**20107/07/27**	**قرار مجلس الادارة رقم 2017/05 بتاريخ 2017/07/27**
02	**2019/09/04**	**قرار مجلس الادارة رقم 2019/05 بتاريخ 2019/09/04**
03	**2021**	**قرار مجلس الادارة رقم 2021/8 بتاريخ 2021/12/23**
04	**2023/04/13**	**قرار مجلس الادارة رقم 2023/2 بتاريخ 2023/04/13**

أولاً: مقدمة

تعد جرائم غسـل الاموال وتمويل الارهاب من أخطر الجرائم الاقتصـادية التي تفاقمت خلال السـنوات الأخيرة، وتعتبر البنوك احدى القنوات المهمة التي تستخدم لغايات تنظيف واخفاء هذه الاموال غير المشروعة المصدر، وإدراكاً من المجتمع الدولي لخطورة الآثار السلبية التي تخلفها عمليات غسل الأموال وتمويل الارهاب على الاقتصادات الوطنية وتهديدها للمجتمع الدولي، فقد توالت الجهود الدولية والإقليمية للحد من هذه الظاهرة والسيطرة عليها وإخضاعها للعقاب وضبط المسؤولين عنها ومعاقبتهم. وتعزيزا للاستقرار المالي في فلسطين وللمحافظة على سلامة الجهاز المصرفي الفلسطيني ، فقد أصدرت السلطة الوطنية الفلسطينية القوانين والتشريعات اللازمة لمكافحة غسل الاموال وتمويل الارهاب، اضافة الى التعليمات الصادرة بالخصوص من الجهات التنظيمية الرقابية ذات العلاقة ، وامتثالاً من البنك الإسـلامي العربي للقانون والتعليمات في مكافحة مثل هذه الجرائم ، قام باسـتحداث دائرة مكافحة غسـل الاموال وتمويل الارهاب لمراقبة الامتثال لأحكام القانون واللوائح والتعليمات والمعايير والقرارات الخاصة بمكافحة غسل الاموال وتمويل الارهاب والتواصل مع وحدة المتابعة المالية بهذا الخصوص .

ثانياً: التعاريف والمصطلحات

لأغراض هذه السياسة تكون للكلمات والعبارات التالية المعنى المبين إزاء كل منها، ما لم تدل القرينة على خلاف ذلك:

1- **البنك**: البنك الإسلامي العربي وكافة فروعه ومكاتبه داخل وخارج فلسطين.
2- **مجلس الادارة**: مجلس ادارة البنك الاسلامي العربي.
3- **لجنة المجلس المختصة**: اللجنة المنبثقة عن مجلس الادارة والتي تشرف على وظيفة مكافحة غسل الاموال وتمويل الارهاب.
4- **المدير العام**: مدير عام البنك الإسلامي العربي.
5- **ضابط الاتصال**: ضابط اتصال مكافحة غسل الأموال وتمويل الارهاب ويرأس دائرة مكافحة غسل الاموال وتمويل الارهاب في البنك.
6- **السياسة**: سياسة مكافحة غسل الاموال وتمويل الارهاب الخاصة بالبنك.
7- **الموظفون**: موظفوا البنك الاسلامي العربي.
8- **السلطات الرقابية**: سلطة النقد الفلسطينية وهيئة سوق رأس المال ومسجل الشركات ووحدة المتابعة المالية .
9- **القانون/ القرار بقانون**: القرار بقانون مكافحة غسـل الاموال وتمويل الارهاب رقم 2022/39 الصـادر عن رئيس السلطة الوطنية الفلسطينية .
10- **المرسوم الرئاسي**: مرسوم رقم(14) لسنة 2022 م بشأن مكافحة غسل الأموال وتمويل الإرهاب الصادر عن رئيس دولة فلسطين بشأن تنفيذ قرارات مجلس الأمن .
11- **وحدة المتابعة المالية** : وحدة مسـتقلة تعمل كوحدة وطنية مركزية لمكافحة جريمة غسـل الاموال وتمويل الارهاب أنشئت بموجب أحكام قانون مكافحة غسل الاموال وتمويل الارهاب وتتبع للجنة الوطنية لمكافحة غسل الاموال وتمويل الارهاب، وتتمتع بصلاحية طلب وتلقي المعلومات من الجهات الملتزمة بأحكام القانون والمراسيم والتعليمات الصادرة بمقتضاه، وتحليلها، وتلقي التقارير اليومية، ويعمل مديرها وموظفيها كوحدة ضابطة قضائية في ممارسة وظائفهم وواجباتهم.

12- **اللجنة الوطنية**: اللجنة المشـكلة لمكافحة جريمة غسـل الأموال وتمويل الإرهاب بموجب أحكام القرار بقانون رقم(20) للعام 2015 .

13- **لجنة تنفيذ قرارات مجلس الأمن الدولي**: اللجنة المشـكلة بقرار من رئيس الدولة وتتولى تنفيذ القرارات الصـادرة عن مجلس الأمن الدولي التابع للأمم المتحدة، بموجب الباب السـابع ذات العلاقة بمكافحة غسـل الأموال وتمويل الإرهاب، وخطر تمويل انتشار أسلحة الدمار الشامل.

14- **الأعمال الارهابية**: جميع الأفعال التي ترمي الى ايجاد حالة ذعر، وترتكب بوسـائل مختلفة كالأدوات المتفجرة والمواد الملتهبة والمنتجات السـامة أو المحرقة، والعوامل الوبائية أو الجرثومية، التي من شـأنها أن تحدث خطراً عاماً، والمنصوص عليها في قانون العقوبات والتشريعات النافذة

15- **الارهابي**: أي شخص يرتكب أي فعل من الأفعال الآتية:

أ. ارتكاب أو الشـروع في ارتكاب أو الاشـتراك كطرف متواطئ في أي من الأعمال الإرهابية بأي وسـيلة سـواء بشكل مباشر أو غير مباشر، وتنظيم أعمال إرهابية أو توجيه الآخرين لارتكابها.

ب. المسـاهمة في ارتكاب الأعمال الإرهابية مع مجموعة من الأشـخاص تعمل لغرض مشـترك، حيث تكون المساهمة متعمدة وبهدف تعزيز العمل الإرهابي أو مع العلم بنية المجموعة في ارتكاب العمل الإرهابي

16- **المنظمة الارهابية**: أي مجموعة من الإرهابيين ترتكب أي من الأعمال الآتية:

أ. ارتكاب أو الشروع في ارتكاب الأعمال الإرهابية عمداً بأية وسيلة بشكل مباشر أو غير مباشر أو التواطؤ في تنفيذ الأعمال الإرهابية أو تنظيم الأعمال الإرهابية أو توجيه الآخرين لارتكابها.

ب. المسـاهمة في ارتكاب الأعمال الإرهابية مع مجموعة من الأشـخاص تعمل لغرض مشـترك، حيث تكون المساهمة متعمدة وبهدف تعزيز العمل الإرهابي أو مع العلم بنية المجموعة في ارتكاب العمل الإرهابي.

17- تمويل الارهاب: يعتبر مرتكباً لجريمة تمويل الارهاب حتى لو لم يقع العمل الارهابي أو لم تستخدم الاموال فعلياً أو لم ترتبط بعمل ارهابي معين، أياً كان البلد الذي يتوجد فيه الشخص، سواء البلد الذي يقع فيه العمل الارهابي أو المنظمة الارهابية، أم في بلد آخر وأياً كان البلد الذي وقع أو سيقع فيه العمل الارهابي:

أ. كل من يقوم عن عمد وبقصد غير مشروع بتوفير الاموال أو جمعها بأية وسيلة سواء كانت مباشرة أو غير مباشـرة، لاسـتخدامها أو مع العلم أنه سـيتم اسـتخدامها جزئياً أو كلياً في ارتكاب أي عمل ارهابي أو من قبل شخص ارهابي أو منظمة ارهابية، أو لغايات سفر أفراد لدولة غير دولة اقامتهم أو جنسيتهم بغرض ارتكاب أو المشاركة أو الاعداد أو تسهيل أعمال ارهابية أو توفير أو تلقي التدريب على أعمال ارهابية.

ب. كل شـخص يحاول ارتكاب جريمة تمويل الارهاب، أو يسـاهم في ارتكاب أو الشـروع في ارتكاب أو يشـارك كطرف متواطئ في أي من جرائم تمويل الارهاب أو ينظم جرائم ارهابية أو يوجه الآخرين لارتكابها أو محاولة ارتكابها منفرداً أو مع مجموعة من الاشـخاص تعمل لغرض مشـترك، أو توفر العلم أو النية بذلك من الظروف الواقعية والموضوعية.

18- **الجريمة المالية**: هي الجرائم التي نص عليها القانون وتشـمل جرائم غسـل الاموال، تمويل الارهاب، الاحتيال، خرق العقوبات، الجرائم الالكترونية.

19- **الجرائم الأصلية**: هي أية جريمة منصوص عليها في قانون مكافحة غسل الاموال وتمويل الارهاب وقوانين العقوبات النافذة وأية قوانين أخرى نافذة في فلسطين

20- **جريمة غسل الاموال وتمويل الارهاب**: وفق القانون الفلسطيني هي " كل سلوك يقصد به إخفاء أو تغير هوية الأموال المتحصلة من إحدى الجرائم الأصلية وذلك تمويهًا لمصادرها الحقيقية لتبدو في ظاهرها متأتية من مصادر مشروعة"، أي أنها عملية إضفاء صفة الشرعية على أموال متأتية من مصدر غير شرعي، وذلك من خلال إدخالها في الدورة المالية الداخلية أو العالمية عبر القنوات المصرفية والمالية وإعادة تدويرها، ويعد مرتكباً لجريمة غسل الأموال كل من قام عمداً أياً من النشاطات التالية و لا تحول معاقبة مرتكب الجريمة الأصلية دون معاقبته على جريمة غسل الأموال:

أ. تحويل الأموال أو نقلها مع العلم بأنها عائدات جريمة أو أي فعل من أفعال المشاركة في مثل هذه الجريمة بقصد إخفاء أو تمويه المصدر غير المشروع لتلك الأموال أو مساعدة أي شخص يرتكب مثل هذه الجريمة على التهرب من العواقب القانونية.

ب. إخفاء أو تمويه الطبيعة الحقيقية للأموال أو مصدرها أو مكانها أو طريقة التصرف فيها أو حركتها أو ملكيتها أو الحقوق ذات الصلة مع العلم بأنها عائدات جريمة.

ت. اقتناء الأموال أو حيازتها أو استخدامها مع العلم بأنها متحصلات إجرامية وقت استلامها.

ث. المشاركة أو تكوين الجمعيات أو التواطؤ أو المساعدة أو التحريض أو التسهيل أو تقدي م المشورة أو التعاون أو المساهمة أو التآمر في ارتكاب أي من الأفعال المنصوص عليها في القانون.

21- **العناية الواجبة (CDD):** Customer Due Diligence ، ويقصد بها مجموعة القواعد المثلى لمتطلبات التعامل مع العميل، بما يشمل التعرف على هويته العميل واوضاعه القانونية ونشاطه ومصدر الاموال والغاية من علاقة العمل وطبيعتها والمستفيد الحقيقي (ان وجد) والتحقق من كل ذلك والمتابعة المتواصلة للعمليات التي تتم في اطار علاقة عمل مستمرة باي وسيلة من الوسائل المحددة بمقتضى التشريعات ذات العلاقة بالاضافة الى التعرف على طبيعة العلاقة المستقبلية فيما بين البنك والعميل والغاية منها.

22- **العناية الواجبة المعززة (EDD):** Enhance Due Diligence العناية الواجبة المعززة، وهي عبارة عن اجراء تحقق وحيطة اضافية تهدف الى التعرف على هوية العميل والتحقق من ان انشطتهم واموالهم شرعية وقانونية والحصول على المستندات المعززة لذلك.

23- **العناية الواجبة المتواصلة (On Going Due Diligence) :هي دراسة العمليات المنفذة خلال علاقة العمل والغرض منها للتأكد من توافقها مع المعلومات عن عملائها من حيث طبيعة نشاطهم وتصنيف مخاطرهم ومصدر الاموال ، وكذلك من تحديث مستنداتهم باستمرار.**

24- **(FATF) Foreign Action Task Force):** مجموعة العمل المالي التي تأسست عام 1989 وتعتبر هذه المجموعة هيئة دولية معنية بوضع السياسات وتحديد معايير مكافحة غسل الاموال واجراءات مكافحة تمويل الارهاب على مستوى العالم.

25- **القوائم المعتمدة** : هي قوائم الحظر الدولية والمحلية والتي تعنى بتصنيف الاشخاص المعرف عليهم دوليا ومحليا بتهم الارهاب وتجارة المخدرات وغسل الاموال والذين يحظر التعامل معهم ، وتشمل (OFAC / UN / EU / ISRAELI / FRENCH / LOCAL LISTS) وأي قائمة اخرى يتم اعتمادها حسب القوانين والتعليمات .

26- **الاحتيال:** أية ممارسة تنطوي على استخدام الخداع للحصول المباشر أو غير المباشر على شكل من أشكال الاستفادة المالية لمرتكب الجريمة، أو تسهيل ذلك لغيره لتؤدي الى شكل من أشكال الخسارة للطرف الذي تعرض للاحتيال، ووفق ما نصت عليه سياسة مكافحة الفساد والرشوة.

27- **المعرض سياسيا:** الشخص المعرض سياسياً وأفراد عائلته وذوي الصلة به وشركائه، الذي شغل أو يشغل في فلسطين أو خارجها مناصب سياسية عامة أو وظائف عليا حسب ما ورد بالقانون والتعليمات ذات العلاقة.

28- **المستفيد الحقيقي/ المالك المنتفع**

أ. **فيما يتعلق بالحساب: هو** الشخص الطبيعي الذي يملك الحساب أو يسيطر عليه بصورة نهائية

ب. **فيما يتعلق بالعملية:** هو الشخص الطبيعي الذي ينفذ العملية أو الشخص الذي يتم تنفيذ العملية بالنيابة عنه (سواء عن طريق التوكيل أو التفويض أو أي شكل آخر من أشكال التفويض

ت. فيما يتعلق الشخص القانوني أو الترتيب القانوني :هو الشخص الطبيعي الذي يمارس سيطرة فعالة ونهائية على شخص اعتباري أو ترتيب قانوني.

29- **العميل:** أي شخص أو كيان يحتفظ بحساب وله علاقة تجارية أو له ارتباط بمعاملة مالية مع البنك. أو هو المستفيد الرئيسي من المعاملات التي تتم من خلال مفوض عن الحساب.

30- **العميل العارض:** العميل الذي لا تربطه بالمصرف علاقة عمل مستمرة.

31- **بنوك الظل (البنوك الوهمية):** البنوك التي ليس لها وجود مادي في الولاية القضائية التي تم ترخيصها فيها والتي لا تنتمي إلى مجموعة مالية منظمة تخضع لإشراف موحد وفعال

32- **علاقة العمل:** العلاقة التي تنشأ بين العميل والبنك وتكون وثيقة الصلة بالنشاطات والخدمات التي يقدمها البنك للعملاء.

33- **الطرف الثالث:** عندما يعتمد أو يفوض البنك مؤسسة مالية أو وسيط آخر، أي جزء من إجراءات العناية الواجبة، يُشار إلى ذلك باسم" الطرف الثالث."

34- **الاصول الافتراضية:** تمثيل رقمي للقيمة أو الحقوق التي يمكن تداولها أو تحويلها أو تخزينها الكترونياً، ويمكن استخدامها لغايات الدفع أو الاستثمار، ولا تشمل التمثيل الرقمي للعملات الرسمية والأوراق المالية وغيرها من الأصول المالية.

35- **المؤسسة المالية:** أي مؤسسة تتولى واحدًا أو أكثر من الأنشطة أو العمليات المدرجة بالقانون والتعليمات ذات العلاقة لمنفعة أو نيابة عن عميل

36- **العقوبات:** هي إجراءات قانونية تفرضها الدول (أو مجموعات البلدان) والكيانات فوق الوطنية(التحالفات الدولية التي تتجاوز فيها قوة الدول ونفوذها الحدود الوطنية)التي تحظر أو تقيد معاملات معينة تخضع لولايتها القضائية التي تشمل حكومات أو أفرادًا أو كيانات محددة أو مرتبطة ببلدان أو أنشطة معينة.

37- **المنظمة غير الهادفة للربح:** أي كيان أو شخص اعتباري أو ترتيب قانوني أو منظمة تشارك بشكل أساسي في جمع الأموال أو توزيعها لأغراض خيرية أو دينية أو ثقافية أو تعليمية أو اجتماعية أو أخوية أو أغراض مماثلة أو تنفذ أشكال أخرى من الأعمال الخيرية أو الأعمال المماثلة.

38-**الولاية القضائية:** أي نوع من أنواع الولاية القضائية القانونية والتي قد تشمل الدولة أو دولة أجنبية (سواء كانت ولاية قضائية مستقلة ذات سيادة أم غيرها) أو دولة أو مقاطعة أو إقليم آخر لدولة أجنبية أو أي سلطة مماثلة.

39-**حسابات الدفع المراسلة:** حسابات المراسلة التي يتم استخدامها مباشرة من قبل أطراف ثالثة لممارسة أعمال لصالحها

40- **المقيم:** الشخص الطبيعي المقيم وفقاً لتعليمات سلطة النقد الفلسطينية رقم (2009/9) الصادرة بتاريخ 2009/12/28، ولإغراض هذه السياسة هو الشخص الذي يقيم داخل فلسطين لمدة عام (بشكل دائم أو مُنقطع) أو أكثر بغض النظر عن جنسيته.

41- **العميل غير المقيم:** الأشخاص الذين لا ينطبق عليهم أي من الشروط أعلاه سواء طبيعي أو اعتباري.

42- **مؤشر الاشتباه:** الحركات التي تجري على حساب العميل أو السلوك الذي يصدر عنه، ويتنافى مع معطيات حسابه وبياناته وطبيعة نشاطه.

43- **تقرير الاشتباه:** هو الاخطار المرسل من قبل البنك الى لوحدة المتابعة المالية عن أية عملية أو نشاط مشتبه به

44- **المؤسسات غير الربحية:** هي المؤسسات المحلية و / او الدولية والتي تعمل داخل فلسطين، ولا تهدف للربح المادي وتختص بتقديم خدمات اجتماعية او انسانية

45- **علاقات المراسلة:** علاقة العمل مع / من خلال بنوك مراسلة عالميه او من خلال بنوك في دول الجوار.

46- **الترتيب القانوني** : الصناديق الاستئمانية المباشرة أو أي ترتيبات قانونية مماثلة كالوقف .

47- **الصندوق الاستئماني:** العلاقات القانونية التي تنشأ بين الأحياء أو عند الوفاة، من قبل شخص أو موصي، عندما تكون الأموال قد تم وضعها تحت سيطرة الوصي وذلك لصالح مستفيد أو لغرض معين، بحيث تشكل تلك الأصول أموالاً مستقلة وليست جزءاً من أملاك الوصي، ويبقى الحق في أصول الصندوق الاستئماني باسم وصي أو باسم شخص آخر نيابة عنه، ويتمتع بالسلطة لادارة واستخدام والتصرف بالأصول طبقاً لشروط الصندوق الاستئماني والواجبات الخاصة المفروضة عليه قانوناً والصلاحيات الممنوحة له.

48- **الصندوق الاستئماني المباشر:** الصندوق الاستئماني الذي ينشئه شخص أو موصي بشكل واضح وصريح، والذي يكون عادة في شكل وثيقة مثل صك استئمان كتابي، وهذا الصندوق يختلف عن الصناديق الاستئمانية في الحالات التي تنشأ من خلال تنفيذ القانون ولا تنتج من قصد الموصي أو الشخص أو قراره الواضح والصريح بانشاء صندوق استئماني أو ترتيبات قانونية مماثلة مثل الصناديق الاستئمانية المنشأة بأحكام قضائية

49- **الوسائط:** أي أموال أو أداة تستخدم أو يقصد إستخدامها بأي شكل سواء بكل كلي او جزئي لغسل الاموال او لتمويل الارهاب أو لارتكاب اي من الجرائم الاصلية.

50- **الحجز التحفظي:** الحظر المؤقت على نقل الاموال او تحويلها او التصرف فيها استنادا لقرار المحكمة المختصة أو اي جهة مخولة بموجب احكام هذا القانون وبما يشمل المتحصلات او الوسائط التي تكون قد استخدمت او كان يقصد استخدامها لأي من الجرائم الاصلية.

51- **التجميد:** حظر نقل الاموال أو الاصول الأخرى أو المعدات أو الوسائط الأخرى أو تحويلها أو التصرف فيها أو تحريكها عندما تكون ملكاً أو يتحكم يها أشخاص أو كيانات مدرجة بناء على اجراءات يبادر الى اتخاذها مجلس الامن أو وفقاً لقرارات مجلس الامن ذات الصلة المطبقة من قبل اللجنة وخلال مدى سريان تلك الاجراءات والقرارات.

ثالثا: الأهداف المتوخاة من هذه السياسة:

تتمثل الأهداف الرئيسية لهذه السياسة فيما يلي :

1.1. بيان المعايير الأساسية لمنع استخدام البنك الاسلامي العربي ومنتجاته وخدماته في عمليات غسيل الأموال و/أو تمويل الإرهاب.

1.2. ضمان التزام البنك في جميع الاوقات بالتشريعات والقوانين والتعليمات المتعلقة بغسل الاموال وتمويل الارهاب.

1.3. مساعدة موظفي البنك في العمل بموجب القوانين والتعليمات النافذة في فلسطين المتعلقة بغسل الاموال وتمويل الارهاب، وعدم خرقها أو انتهاكها، والتعامل بشكل فعال مع الجرائم الأصلية المتعلقة بها والإبلاغ عنها حسب التعليمات والاجراءات المعتمدة.

1.4. تعزيز أفضل الممارسات لحماية البنك من الخسائر المالية والأضرار التي تلحق بالسمعة التي قد تنشأ عن التورط في جريمة متعلقة بغسل الأموال و/أو تمويل الإرهاب.

1.5. تحديد إطار عمل لتمكين البنك من تحديد والإبلاغ عن أي نشاط مشبوه يتعلق بغسل الأموال و / أو تمويل الإرهاب لوحدة المتابعة المالية.

رابعا: نطاق التطبيق والامتثال للسياسة والاطلاع عليها:

1. نطاق التطبيق:

1/1 تتضمن هذه السياسة الحد الأدنى من المعايير والقواعد الواجب تطبيقها والعمل بموجبها في البنك بأكمله، وتسري على جميع دوائر وفروع البنك ومكاتبه المصرفية والتمثيلية.

2/1 كما تنطبق على التحالفات والشراكات الإستراتيجية التي يتم ابرامها مع البنك، ولا تنطبق على الكيانات التي ليس للبنك فيها سيطرة قانونية أو تشغيلية.

3/1 تتوافق هذه السياسة مع سياسة الشركة الام "بنك فلسطين " واطارها العام، ولأغراض مكافحة غسل الاموال وتمويل الارهاب وادارة المخاطر المتعلقة بها في البنكين.

2. الامتثال للسياسة:

2.1. يجب على جميع موظفي البنك الامتثال لهذه السياسة، والعمل بموجبها في جميع الأوقات، وفي حال عدم الامتثال لها أو تجاهلها سواء عن عمد أو بالتقصير واللامبالاة والاهمال، سوف يتعرض المخالفون للإجراءات التأديبية وفقاً لأحكام نظام موظفي البنك ولائحة عقوباته التأديبية، والذي قد يصل لحد انهاء الخدمات وفقاً لمدى المخاطر الناتجة عن المخالفة.

2.2. الموظف/ الموظفون الذين يتم توجيه تنبيه أو عقوبة معينة لهم فيما يتعلق بخرق هذه السياسة أو عدم الامتثال لها، يخضعون لإعادة تأهيل وتدريب لتجنب تكرار المخالفة، مع التوقيع على تعهد خطي بعدم المخالفة مرة أخرى.

2.3. يجب ابلاغ ضابط اتصال مكافحة غسل الاموال وتمويل الارهاب بأي خرق أو مخالفة أو الشك بحدوثهما فيما يتعلق بقواعد ومبادئ هذه السياسة حسب سياسة واجراءات الابلاغ الداخلي المعتمدة في البنك.

2.4. أي انحراف عن تطبيق هذه السياسة او إنفاذها استثناء، يجب توثيقه وابلاغ لجنة المجلس المختصة.

3. الاطلاع وتداول السياسة:

3.1. تعامل هذه السياسة على أنها وثيقة سرية ولا يجوز الكشف عنها أو توزيعها لأي شخص طبيعي أو اعتباري، ولا يجوز الاطلاع عليها أو توزيعها أو نسخها من قبل أي شخص طبيعي أو اعتباري غير مخول دون موافقة خطية من ضابط اتصال مكافحة غسل الاموال وتمويل الارهاب.

3.2. أي طرف ثالث يحصل على نسخة من هذه السياسة سواء الكترونية أو غيرها، يجب أن يوقع على تعهد بعدم التصرف فيها أو اعادة توزيعها أو اطلاع آخرين عليها دون اذن خطي من البنك قبل استلام أي نسخة منها.

3.3. تستخدم نسخة غير قابلة للتحرير (Hard copy) لأغراض الاطلاع والتوزيع، وتحتفظ دائرة مكافحة غسل الاموال وتمويل الارهاب بالنسخة (Word) اضافة لدائرة التنظيم واجراءات العمل.

خامساً: المرجعية القانونية والتنظيمية للسياسة:

تم اعداد هذه السياسة بحيث تأخذ بالاعتبار القوانين والتشريعات والتعليمات والانظمة والتوجيهات الصادرة عن الجهات ذات الاختصاص والتوصيات والاطر العالمية. (ملحق رقم 1)

سادساً: مراحل جريمة غسل الاموال وتمويل الارهاب:

يقصد بها الآليات أو العمليات التي يقوم بها غاسلوا الأموال لاخفاء المصدر غير الشرعي للاموال أو لتمويل الارهاب، والتي تمر عبر 3 مراحل، وتحتوي كل مرحلة على عدد من العمليات. (ملحق رقم 2)

سابعاً: حوكمة وظيفة غسل الاموال وتمويل الارهاب:

1. خطوط الدفاع الثلاثة:

تقع مسؤولية الدفاع عن البنك في مواجهة مخاطر غسل الاموال وتمويل الارهاب على عاتق الحلقات أو خطوط الدفاع المتتالية التالية:

أ. **خط الدفاع الأول: دوائر ووحدات الأعمال والعمليات التشغيلية:** وهي التي تقوم بالأعمال والانشطة التنفيذية المختلفة في البنك، وتعتبر خط الدفاع الاول في البنك، وبالتالي تقع المسؤولية الأولى عليها في تحديد وادارة المخاطر في البنك، والعمل بموجب القوانين واللوائح والانظمة والسياسات والتعليمات، والالتزام بالضوابط الرقابية المختلفة على العمليات التي تقوم بها، ويكون رئيس كل وحدة / دائرة أعمال مسؤولاً عن توضيح أهمية ومتطلبات هذه السياسة وتطبيقها وتوجيه موظفيه للالتزام باجراءات التعرف على العميل وتوثيقها وتنفيذ سياسة اعرف عميلك.

ب. **خط الدفاع الثاني: وظائف الامتثال وادارة المخاطر:** حيث تقوم هذه الوظائف بالتحقق من امتثال البنك وادارة مخاطره، وتتمثل في دائرة مراقبة الامتثال، دائرة مكافحة غسل الاموال وتمويل الارهاب، دوائر ادارة المخاطر، حيث تقوم بتحديد وقياس ومتابعة المخاطر في نطاق مهامها، وترفع التقارير بشأنها بشكل مستقل عن خط الدفاع الاول إلى مجلس الادارة/ لجنة مجلس الادارة المختصة ورفع التوصيات بشأن انهاء علاقة عمل أو إيقاف أنشطة ذات مخاطر مرتفعة ولا تتماشى مع المتطلبات الرقابية أو سياسة قبول المخاطرة لدى البنك (شهية المخاطر).

ت. خط الدفاع الثالث: وظيفة اعطاء التوكيد المستقل:

وتتمثل في وظيفة التدقيق الداخلي والتي يجب أن تقوم بمراجعة مدى فعالية الإجراءات وأنظمة الرقابة المطبقة فيما يتعلق بمكافحة غسل الأموال وتمويل الإرهاب على أساس سنوي باستخدام نهج قائم على المخاطر، ويجب أن تقدم توصياتها لسد أي ثغرات وتحديد الإجراءات اللازمة لضمان فعاليتها وكفايتها، وتشمل عملياتها تقييم الهياكل والسياسات والإجراءات وتنفيذ الدوائر لمعايير البنك الخاصة بمكافحة غسل الأموال وتمويل الإرهاب وإدارة مخاطر العقوبات.

2. الأدوار والمسؤوليات الرئيسية في مكافحة غسل الاموال تمويل الارهاب في البنك:

أ. مجلس الإدارة:

أ.1. ضمان فعالية السياسات والاجراءات والانظمة والضوابط في منع غسل الاموال وتمويل الارهاب وتبني النهج القائم على المخاطر بالاستناد الى توصيات مجموعة العمل المالي والممارسات الدولية والمبادئ التوجيهية للجنة بازل.

أ.2. انشاء وظيفة مستقلة لمكافحة غسل الاموال وتمويل الارهاب، لتنفيذ الضوابط والاجراءات اليومية لمنع غسل الاموال وتمويل الارهاب والحفاظ على سياسات واجراءات وأنظمة وضوابط فعالة لمكافحة غسل الاموال وتمويل الارهاب، وتوفير الموازنات والموارد اللازمة لها، والصلاحيات التي تمكنها من أداء عملها بما في ذلك الوصول غير المقيد لجميع المعلومات ذات الصلة بالوظيفة، وضمان استمرارية عمل الدائرة دون انقطاع.

أ.3. اعتماد هيكل تنظيمي واضح لهذه الوظيفة يتناسب مع حجم البنك وتفرعاته وتعقد عملياته وقاعدة عملائه واعتماد الاوصاف الوظيفية للدائرة ونظام مكافآت وحوافز موظفي الدائرة.

أ.4. التأكد من وجود رئيس للدائرة يتمتع بالمواصفات والخبرات والمؤهلات وفق تعليمات سلطة النقد، وعدم تكليفه أو انخراطه في عمل تنفيذي من شأنه ان يؤدي تعارض في المصالح.

ب. اللجنة المختصة المنبثقة عن مجلس الادارة:

ب.1. مساعدة مجلس الادارة في القيام بمسؤولياته والعمل كمستشار للمجلس في الامور المتعلقة بمخاطر غسل الاموال وتمويل الارهاب.

ب.2. الاشراف على وظيفة مكافحة غسل الاموال وتمويل الارهاب، واعتماد خططها السنوية

ب.3. الاطلاع على تقارير الدائرة ومناقشتها ورفع التقارير للمجلس عند الحاجة

ت. الادارة العليا:

ت.1. ضمان تنفيذ الدائرة لأنشطة مكافحة غسل الاموال وتمويل الارهاب وتوفير كافة الوسائل والادوات اللازمة لها للقيام بمهامها ومسؤولياتها.

ت.2. التأكد أن البنك لديه برامج تدريب مناسبة ومستمرة لموظفي البنك في مكافحة غسل الاموال وتمويل الارهاب.

ث. دائرة مكافحة غسل الاموال وتمويل الارهاب:

ث.1. مسؤوليات الدائرة:

ث.1.1. ابلاغ وحدة المتابعة المالية بتقارير الإشتباه بجرائم غسل الأموال وتمويل الارهاب ومتابعة الرد على طلباتها.

ث.1.2. استلام الابلاغات من اي من موظفي المصرف إذا توافر لدى الموظف الشك في ان العملية المراد تنفيذها هي عملية يشتبه يارتباطها بغسل الاموال او تمويل الارهاب او اي من الجرائم الاصلية.

ث.1.3. متابعة وتنسيق البرامج التدريبية الخاصة بمكافحة غسل الأموال وتمويل الارهاب لموظفي البنك.

ث.1.4. التأكد من مدى التزام البنك بأحكام قرار قانون مكافحة غسل الأموال وتمويل الإرهاب والتعليمات الصادرة بموجبه، ورفع التقارير الدورية للجنة المجلس المختصة.

ث.1.5. مراقبة العمليات النقدية والحوالات والمعاملات الإئتمانية والإستثمارية وذلك عن طريق استخدام نظام آلي.

ث.1.6. متابعة قوائم أسماء المشبوهين وما يتم عليها من تعديلات، وفق المعايير الدولية ذات العلاقة.

ث.1.7. تصنيف عملاء المصرف وفقاً لدرجة مخاطرهم (مرتفعة، متوسطة ، منخفضة) والإستمرار بمراقبة العملاء ذوي المخاطر المرتفعة والمتوسطة.

ث.1.8. الإحتفاظ بالسجلات والدراسات والمعلومات عن كافة البيانات الخاصة بجميع العمليات المشبوهة وغير العادية.

ث.1.9. التأكد من التزام كافة موظفي المصرف من تطبيق قاعدة اعرف عميلك بمختلف مستوياتها ومتطلباتها.

ث.1.10. تحديد آليات إنشاء علاقات العمل وآليات قبول أو رفض العملاء.

ث.2. **<u>مسؤوليات مدير الدائرة:</u>**

ث.2.1. اعداد سياسات واجراءات الدائرة ومراجعتها وتحديثها.

ث.2.2. المشاركة في وضع وتنسيق البرامج التدريبية الخاصة بنشاط الدائرة.

ث.2.3. إعداد الخطة السنوية للدائرة.

ث.2.4. تطوير وتحديث نموذج تقييم مخاطر العملاء.

ث.2.5. التقييم السنوي على الأقل لمخاطر الجرائم المالية على مستوى المؤسسة.

ث.2.6. القيام بالدور استشاري لخط الدفاع الأول فيما يتعلق بمخاطر غسل الأموال وتمويل الإرهاب.

ث.2.7. التحقق من الامتثال لهذه السياسة من خلال برنامج متابعة خاص لاختبار فعالية وكفاءة ضوابط الامتثال.

ث.2.8. تقييم مدى كفاية سياسات وإجراءات البنك فيما يتعلق بمكافحة غسل الأموال وتمويل الإرهاب.

ث.2.9. مراجعة تصنيف درجة تعرض العملاء لمخاطر غسل الاموال وتمويل الارهاب.

ث.2.10. قيادة التقييم الذاتي لمخاطر غسل الاموال وتمويل الارهاب في البنك.

ث.2.11. اعداد تقارير دورية نصف سنوية / على الاقل / واحصائية عن عمل الدائرة وكافة العمليات غير العادية والمشتبه بها

ج. <u>دائرة مراقبة الامتثال:</u>

التنسيق مع مع دائرة مكافحة غسل الاموال وتمويل الارهاب فيما يتعلق بما يلي:

ج.1. الحسابات التي تشير الى ممارسة أعمال الصرافة للتأكد من امتثال الفروع للتعليمات ذات العلاقة

ج.2. الحسابات ذات الصلة بقانون الامتثال الضريبي الامريكي للحسابات الخارجية، وحسابات المنظمات غير الهادفة للربح.

ج.3. الانتهاكات أو الاخفاقات في الامتثال لاجراءات مكافحة غسل الاموال وتمويل الارهاب

ج.4. التعليمات الجديدة أو التحديثات على التعليمات القائمة بخصوص مكافحة غسبل الاموال وتمويل الارهاب.

ج.5. الاشخاص المعرضين سياسياً

ح. <u>ادارة المخاطر:</u>

التنسيق والتواصل فيما يتعلق بمخاطر غسل الاموال وتمويل الارهاب وضوابط الاحتيال لاتخاذ الاجراءات اللازمة للتخفيف من المخاطر

خ. <u>ادارة تكنولوجيا المعلومات/ دائرة انظمة الاعمال المصرفية:</u>

خ.1. توفير البرامج الآلية التي تدعم وتساند عمل وحدة مكافحة غسل الأموال وتمويل الارهاب عند طلبها

خ.2. توفير أية تقارير يتم طلبها من مكافحة غسل الأموال وتمويل الارهاب عند الطلب.

خ.3. التعاون مع وحدة مكافحة غسل الاموال وتمويل الارهاب لتطبيق معايير تصنيف العملاء حسب درجة المخاطرة على النظام البنكي.

خ.4. اجراء التعديلات على البرامج و/أو التقارير لتتوافق ومتطلبات مكافحة غسل الأموال وتمويل الارهاب.

خ.5. تحديث قوائم OFAC و UN list بالاضافة الى اي قوائم يتم اعتمادها من قبل البنك على النظام البنكي وبشكل دوري وفور اجراء اي تحديثات عليها من مصدرها.

خ.6. التعاون مع دائرة مكافحة غسل الأموال وتمويل الارهاب بشأن التدريب على أية برامج مستجدة واجابتها حول أية استفسارات فنية بالخصوص.

خ.7. التحديث اليومي للقوائم السوداء من خلال الموقع المخصص لذلك وطباعة نتيجة التحديث وحفظه "للتوثيق"

د. <u>ادارة الموارد البشرية/ التدريب:</u>

د.1. تنسيق مع دائرة مكافحة غسل الأموال وتمويل الارهاب بشأن خطة التدريب لموظفي وحدة مكافحة غسل الأموال وتمويل الارهاب.

د.2. التنسيق مع دائرة مكافحة غسل الأموال وتمويل الارهاب بشأن الخطط التدريبية لموظفي البنك في مجال مكافحة غسل الأموال وتمويل الإرهاب

ذ. <u>ادارة التدقيق الداخلي:</u>

ذ.1. مراجعة كافة الضوابط والإجراءات المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب.

ذ.2. إخطار دائرة مكافحة غسل الأموال وتمويل الإرهاب بأي خلل أو انتهاكات أثناء فحص تطبيق الإجراءات اللازمة أو عندما تكون أنظمة الرقابة على مكافحة غسل الأموال وتمويل الإرهاب عرضة للخطر•

ذ.3. تقييم الوعي مكافحة غسيل الأموال وتمويل الإرهاب بين موظفي البنك.

ذ.4. التأكد من امتثال الفروع للاجراءات واللوائح المحددة أثناء فتح الحسابات وإخطار دائرة مكافحة غسل الأموال وتمويل الإرهاب بأي فشل في الأداء.

ذ.5. إخطار دائرة مكافحة غسل الأموال وتمويل الإرهاب بأي مؤشرات مشبوهة أثناء جولات التفتيش الميداني

ذ.6. فحص أنظمة وبرامج مكافحة غسل الأموال وتمويل الإرهاب بشكل منتظم والتأكد من سلامة الضوابط الأساسية.

ر. **وحدة علاقات المساهمين:**

عدم السماح باستقطاب مساهمين جدد يشتبه بارتكابهم جرائم غسل اموال او تمويل ارهاب وابلاغ دائرة مكافحة غسل الاموال بالخصوص .

ز. **الدائرة القانونية:**

ز.1. تفسير المتطلبات القانونية التي لها علاقة بقانون مكافحة غسل الاموال وتمويل الارهاب والتعليمات الصادرة بموجبه.

ز.2. تقديم النصح والارشاد في القضايا المتعلقة بمكافحة غسل الاموال وتمويل الارهاب.

س. **الموظفون:**

س.1. الإلتزام بالقوانين واللوائح والتعليمات وقواعد السلوك ومعايير الممارسات المهنية السليمة المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب.

س.2. الإلتزام باستيفاء المعززات للعمليات المالية التي تتم على حسابات العملاء وفقاً لتعليمات خاصة تصدر بموجب هذه السياسة من قبل الجهات ذات العلاقة وحسب الاصول .

س.3. الإبلاغ بوجه السرعة عن أي نشاط أو عملية يشتبه بأنها تنطوي على جريمة أصلية أو جريمة غسل أموال أو تمويل للإرهاب.

س.4. عدم الإفصاح للعملاء أو أي طرف ثالث بأنه جرى تقديم معلومات لوحدة المتابعة المالية أو بأنه تم رفع تقرير يتعلق بالإشتباه في جريمة غسل الأموال أو تمويل الإرهاب أو أي من الجرائم الأصلية أو سيتم إجراؤه.

س.5. الرد على مراسلات وحدة مكافحة غسل الأموال وتمويل الارهاب وفقاً للمهلة الممنوحة من قبل وحدة مكافحة غسل الأموال وتمويل الارهاب.

س.6. حضور التدريب وورش العمل بشأن مكافحة غسل الأموال وتمويل الإرهاب ومتطلبات اعرف عميلك.

ثامناً: النهج القائم على المخاطر:

طرأ على قواعد وسبل واجراءات مكافحة غسل الاموال وتمويل الارهاب تغييرات ومستجدات دولية واقليمية ومحلية بالغة الاهمية، تمثل أهمها في تبني توصية مجموعة العمل المالي (FATF)، بشأن تطبيق النهج القائم على المخاطر كنظام فعال لمكافحة غسل الاموال وتمويل الارهاب، وتركيز الجهود لمعالجة أوجه القصور مرتفعة المخاطر، بحيث تطبق تدابير مبسطة في حال المخاطر المنخفضة، لذلك وتماشياً مع توصيات الفاتف وتعليمات سلطة النقد الفلسطينية والممارسات الدولية، فقد تبنى البنك نهجاً قائماً على المخاطر في مراقبة أعماله وعملائه ومعاملاتهم يقوم على تحديد وتقييم وفهم التهديدات ومخاطر غسل الأموال وتمويل الإرهاب والعقوبات التي قد يتعرض لها، واتخاذ التدابير والضوابط للحد والتخفيف منها، أخذاً بالاعتبار نتائج تقييم الدولة للمخاطر، وكافة عوامل الخطر المتعلقة بالعملاء، الدول، المناطق الجغرافية، المنتجات والخدمات، العمليات وقنوات التسليم، مما يؤدي الى الاستخدام الأكثر كفاءة للموارد، واستخدام الطرق الأكثر فعالية.

يتطلب هذا النهج التعرف على التهديدات، ونقاط الضـــعف والعواقب التي قد تنشـــأ عنهما، ومن ثم اجراء مراجعة شـــاملة لأنظمة وتدابير وضوابط مكافحة غسل الاموال وتمويل الارهاب للتعرف على النقاط المحتمل استغلالها لارتكاب هذه الجرائم ، ويتطلب ذلك ما يلي :

1. تحديد المخاطر التي قد يتحملها البنك في حال انتهاك أو خرق القوانين والأنظمة والتعليمات ذات العلاقة، مثل الغرامات المالية والملاحقات القانونية والمقاطعة ومخاطر الســـمعة وغيرها، والتي تؤثر جوهرياً على البنك وعملائه ومســـاهميه والاطراف ذات العلاقة، بحيث تكون عملية ادارة المخاطر جزءا لا يتجزأ من كافة أنشـــطة البنك، وليس دائرة ادارة المخاطر وحدها ، وأن تتحمل الادارة وجميع الموظفين على جميع المستويات مسؤولية خاصة في تقييم بيئة المخاطر لديهم ووضع الضوابط المناسبة ومراقبة فعالية تلك الضوابط، والتأكيد على ثقافة إدارة المخاطر.
2. تتبع مؤشـــرات المخاطر الرئيســـية ("Krls" Key Risk Indicators) ومراقبتها والإبلاغ عنها لاتخاذ الإجراءات المناسبة والتي تشتمل على نوعين من المؤشرات:

أ. المؤشـــرات النوعية: مثل الشـــفافية، تعقد هيكل الملكية، نوعية الثقافة الخاصـــة بالمخاطر (متحفظة أم تميل للمخاطرة)، مدى الالتزام بالقواعد والضوابط ذات الصلة، سجل العقوبات، والمؤشرات ذات الصلة بسمعة المؤسسة.

ب. المؤشـــرات الكمية: مثل حجم العميل، ســـنوات عمله، نوع العملاء، الموقع الجغرافي، المنتجات والخدمات، قنوات توصيل الخدمات والمنتجات. وتنقسم هذه المؤشرات الى نوعين من المخاطر:

ب.1 مخاطر هيكلية: وهي السمات الهيكلية للمؤسسة أو الشركة التي لا ترتبط بالانشطة التي تمارسها، ولكنها قد تؤثر في تعرضها لمخاطر غسل الاموال وتمويل الارهاب، مثل هيكل الشركة، سنوات عملها.

ب.2 مخاطر النشـاط: وهي تلك المخاطر الناتجة عن العملاء والانشـطة التي يمارسـونها والطبيعة الجغرافية لهم بالاضـافة للمنتجات والخدمات المقدمة لهم، وقنوات تقديمها، وتعد مؤشـرات مخاطر النشـاط مكوناً رئيسـياً لتحليل المخاطر، وتنقسم لأربعة مجموعات فرعية:

ب.2.1 أنواع العملاء والمستفيدين الحقيقيين (الحاليين والمتوقعين)

ب.2.2 المنتجات والخدمات التي يقدمها البنك

ب.2.3 المنطقة الجغرافية للعميل ونشاطه (داخلياً وخارجياً، أخذاً في الاعتبار قوائم مجموعة العمل المالي FATF ومكتب مراقبة الاصـــول الاجنبية OFAC وقوائم الاتحاد الاوربي وغيرها من القوائم المعتمدة لدى البنك)

ب.2.4 قنوات التوصيل المستخدمة (بما في ذلك التقنيات/ التكنولوجيا المستخدمة في تقديم الخدمة، أخذاً بالاعتبار المخاطر المستجدة نتيجة الرقمنة والحلول التكنولوجية حيث يمكن استغلال الوسائل والحلول التكنولوجية والمنصات الالكترونية واساءة استغلال اموال المساعدات الدولية والانسانية وغيرها في جرائم غسل الاموال وتمويل الارهاب)

3. أية مخاطرة يتم قبولها يجب أن تكون وفق ســياســة البنك في قبول المخاطرة Risk appetite التي يجب أن تبنى وفق أفضل المعايير والممارسات الدولية.
4. المخاطر المتأصــلة Inherent Risk والمخاطر المتبقية Residual Risk : يتوجب الاخذ بعين الاعتبار نتائج تقييم مخاطر غســل الاموال وتمويل الارهاب لمنتجات وخدمات البنك واحتســاب تعرضــها لمخاطر غســل الاموال وتمويل الارهاب وفقا للمنهجية المعتمدة ، ومشـاركة النتائج بشـكل سـنوي مع الادارة التنفيذية ولجنة المجلس المختصـة ووضـع

خطة لتخفيض المخاطر ، وتشمل منهجية المخاطر المتاصلة عوامل مخاطرة العقوبات / القوائم السوداء / التعامل مع طرف ثالث / الشفافية / السيولة (التعامل المكثف بالنقد) / سرعة السداد / المعالجة اليدوية للمعاملات .

5. تقييم مخاطر المنتجات والخدمات :

يجب تحديد وتقييم مخاطر غسل الاموال وتمويل الارهاب للمنتجات والخدمات في البنك وفقا لما يلي :

5.1. دائرة مكافحة غسل الاموال وتمويل الارهاب :

5.2. المشـاركة في تحديد وتقييم مخاطر غسـل الاموال وتمويل الارهاب للخدمات والمنتجات الجديدة قبل اطلاقها واجراء تقييم دوري لمخاطر مكافحة غسل الاموال للمنتجات والخدمات القائمة.

5.3. دائرة ادارة المخاطر :

5.4. المشـــاركة في تحديد وتقييم وقياس مخاطر الخدمات والمنتجات الجديدة قبل اطلاقها والتقييم المدروس للخمات والمنتجات القائمة ووضع الضوابط الرقابية اللازمة لتخفيض مخاطرها .

6. التقييم الذاتي للمخاطر:

6.1. يقوم البنك بعملية تقييم ذاتي شامل دوري كل سنتين على الاقل وعند الحاجة، أو عند نشوء حالات أو مخاوف بشأن جرائم مالية قد يمكن حدوثها من خلال شبكة البنك أو قنوات أو آليات الكترونية جديدة أو مستحدثة، لتقييم التهديدات والمخاطر المحتملة واعداد خطة تصويب/ علاج لجوانب النقص أو القصور.

6.2. يقود ضـابط اتصـال مكافحة غسـل الاموال وتمويل الارهاب عملية التقييم الذاتي، ويتم توثيق هذه العملية للمراجعة والتعرف على فعالية الضـــوابط التي يطبقها البنك، والتطور في اتجاهات العلاج والتصـــويب للتخفيف أو الحد من المخاطر.وتقدم وثيقة التقييم الذاتي ونتائجه وخطة التصويب لسلطة النقد عند الطلب.

6.3. تعتمد سياسة التقييم الذاتي على اربعة محاور رئيسية (العملاء 50%/ المواقع الجغرافية 20%/ المنتجات والخدمات 20% / قنوات التوزيع 10%) .

7. <u>تصنيف درجة مخاطرة العميل عند فتح الحساب (انشاء علاقة العمل):</u>

يتم تصنيف درجة مخاطرة العميل عند فتح الحساب الى منخفض/ متوسط/ مرتفع المخاطر، وفقاً للعناصر الرئيسية التالية:

7.1. قوائم الحظر والتجميد:

7.2. العملاء المدرجون بالقوائم يعتبرون مرتفعي المخاطر ولا يتم فتح حسابات لهم.

7.3. المنطقة الجغرافية:

7.4. حيث يتم التعرف على مكان اقامة العميل، مكان التأسـيس والعمليات بالنسـبة للأشـخاص الاعتباريين، ويصـنف الشـخص المقيم في منطقة جغرافية ذات مخاطر مرتفعة والشـركة المسـجلة في بلد مرتفعة المخاطر أكثر خطورة من الانسـان المقيم و/أو المسـجلة في مناطق منخفضـة المخاطر وتعتبر الدولة/ المنطقة مرتفعة المخاطر في حال وجود قصـــور في تطبيق برنامج فعال لمكافحة غســـل الاموال وتمويل الارهاب، أو أنها منطقة تشـــتهر بأنها ذات ملاذ ضريبي، وتتمثل في المناطق التالية:

7.4.1. الدول المصـنفة من قبل الفاتف بأنها دول ذات مخاطر مرتفعة وتعاني من قصـور استراتيجي في نظام مكافحة غسل الاموال وتويل الارهاب، والدول غير المتعاونة.(لا تملك أنظمة كافية).

7.4.2. دول تخضع لعقوبات من قبل الفاتف أو الامم المتحدة.

7.4.3. المناطق الحدودية بين الدول المشهورة بالنزاعات وتمويل الارهاب.

7.4.4. الدول الأكثر فساداً في العالم وفق مؤشر الشفافية العالمي.

7.5. المعلومات العامة حول العميل:

7.6. وتشمل المعلومات أو الأخبار السلبية المنشورة عن العميل (Adverse Media) مثل أن تكون هناك سمعة سلبية للعميل أو أخبار منشورة عن تورطه في قضايا غسل أموال أو تمويل ارهاب حتى وان لم يكن اسمه مدرجاً بقوائم الحظر فيعتبر ذا مخاطر مرتفعة وعالية.

7.7. طبيعة العمل/ النشاط: ويصنف العميل هنا حسب طبيعة عمله أو نشاطه على النحو التالي

7.7.1. القطاع الاقتصادي للعميل، فالعميل الذي يعمل في قطاع المجوهرات يعتبر أعلى مخاطر من العميل الذي يعمل كموظف حكومي.

7.7.2. الشكل القانوني

7.7.3. منصب العميل، فيما اذا كان العميل معرض سياسياً أم لا، فالعميل المعرض سياسياً يعتبر ذا مخاطر مرتفعة أكبر من العميل الذي لا يشغل منصباً سياسياً.

7.7.4. 7.4.4 مصدر الدخل فالعميل ذو مصدر الدخل القليل أقل خطورة من العملاء ذوي مصدر الدخل المرتفع، نظراً لأن العملاء ذوي مصدر الدخل المرتفع يعتبرون أكثر عرضة من حيث درجة التعرض لمخاطر غسل الأموال وتمويل الارهاب.

7.8. الغاية من فتح الحساب (Risk Level of Purpose of Opening Account):

7.9. مثال ذلك ، فإن العميل الذي تكون الغاية من فتح الحساب لديه تلقي الراتب هو عميل ذو مخاطر منخفضة مقارنةً بعميل يفتح الحساب من أجل شراء العملاء الافتراضية مثل البيتكوين وغيرها أو تلقي التبرعات على سبيل المثال.

7.10. طبيعة المنتجات التي يرغب العميل باستخدامها (Risk Level of Products):

7.11. تصنف درجة مخاطرة المنتجات والخدمات اعتماداً على طبيعة المنتج أو الخدمة، فتعتبر مرتفعة في حال عدم امكان الكشف عن هوية العميل، أو تنطوي على التعامل مع كميات كبيرة من العملة أو العملات، وكذلك العمليات العابرة للحدود مثل الشيكات الاجنبية والايداعات النقدية ، ويعتبر العميل الذي يفتح الحساب من أجل التوفير، عميل ذو مخاطر أقل من عميل يقوم بفتح حساب من أجل الحصول على نقاط بيع أو فتح حساب جاري واصدار واستقبال حوالات خارجية.

7.12. مصدر ثروة العميل (Risk Level of Source of Wealth):

7.13. يعتبر مصدر ثروة العميل من التقاعد على سبيل المثال مصدر ثروة منخفضة المخاطر في حين يعتبر الميراث مصدر ثروة عالي المخاطر لصعوبة تتبع مصدر المال.

7.14. القنوات المستخدمة في تنفيذ العمليات المالية(Risk Level of Channels) وتشمل:

7.14.1. الخدمات الالكترونية Online Services: فالعمليات التي تعتمد على القنوات الالكترونية تعتبر مرتفعة المخاطر مثل الانترنت البنكي، الموبايل البنكي، نقاط البيع POS.

7.14.2. فالعميل الذي يعتمد بشكل كبير على تنفيذ معظم حوالاته وحركاته المالية على الصراف الآلي أو من خلال الانترنت البنكي (ليس وجهاً لوجه) يعتبر عميل ذو مخاطر أعلى من العميل الذي يعتمد بشكل أقل على القنوات الالكترونية.

7.14.3. خدمات أو قنوات الاتصال التي لا تتطلب تعامل بشكل مباشر مع العميل (عدم وجود علاقة مباشرة وجهاً لوجه مع العميل)

7.14.4. الوكلاء

7.14.5. شركات الوساطة المالية

7.14.6. أطراف ثالثة (مثل شركات الاتصالات)

7.15. مخاطر مستجدة:

7.15.1. عمليات الاحتيال التي تتجنب تدابير العناية الواجبة وخاصة عند القيام بتأسيس علاقة العمل، أو من خلال استغلال أشخاص آخرين في علاقة العمل، بالاضافة لجمع التبرعات لأغراض غير مشروعة وعقد صفقات طبية وهمية باستخدام المنتجات والخدمات المالية مثل خطابات الضمان والاعتمادات المستندية، والاحتيال في مجال الاستثمار وخاصة تجارة المستلزمات الطبية.

7.15.2. استغلال الوسائل الالكترونية مثل المنصات الالكترونية لاخفاء المصادر التي قد تكون غير مشروعة في التدفقات النقدية والحوالات المالية، بالاضافة لاستغلال بعض العملاء وخاصة كبار السن في عمليات الاحتيال عبر الانترنت وامكانية انشاء حسابات وهمية لشركات تعمل في المجال الطبي، وامكانية وضع برامج على الهواتف المحمولة وأجهزة الحاسب الآلي واستغلالها في الدخول الى حسابات الاشخاص المصرفية، وقيام بعض المجرمين بارسال رسائل وهمية واستغلال العملاء في الحصول على بياناتهم المالية.

7.15.3. اساءة استخدام الاموال الحكومية أو المساعدات الدولية والانسانية، واختلاس المساعدات أو سوء ادارتها.

7.15.4. استغلال الحالات الانسانية والأوضاع العالمية لجمع الاموال لتمويل الارهاب، واساءة استخدام الخدمات التي تقدمها الجهات غير الهادفة للربح.

7.15.5. استغلال التقلبات في القطاع المالي والاوضاع الاقتصادية للمؤسسات المالية والشركات لاخفاء المتحصلات الاجرامية في الانشطة الاقتصادية المشروعة بشراء المشروعات قيد التصفية وغيرها.

7.15.6. الحركات الفعلية والمتوقعة على الحساب .

8. <u>التصنيف بعد فتح الحساب:</u>

بعد فتح الحساب، يتم مراقبة حركة حساب العميل، ومن ثم تحديد عوامل الخطر أثناء دورة حياة حساب العميل، واحتساب درجة مخاطرة العميل الكلية والتي قد تتغير مثلا من منخفض المخاطر الى متوسط أو مرتفع المخاطر أو العكس، بناءً على عدة عوامل أخرى خلاف العوامل التي تم بناء عليها تقييم وتصنيف درجة مخاطرة العميل ابتداءً عند فتح الحساب، ومنها على سبيل المثال لا الحصر:

8.1.حركة الحساب والعمليات التي تتم عليه، والتنبيهات التي تتعلق بعمليات غير اعتيادية على الحساب ومدى تناسبها مع ما تم التصريح به أثناء فتح الحساب.

8.2.الشك بصحة البيانات.

8.3.تغيير مهنة العميل إلى مهنة ذات مخاطر مرتفعة.

9. شهية المخاطر Risk Appetite وسياسة القبول :

9.1.شهية المخاطر: تتلخص شهية المخاطر لدى البنك في القواعد الاساسية التالية:

9.1.1. عدم التسامح مطلقاً مع حالات عدم الامتثال والانتهاكات للانظمة والتعليمات التي تعرض البنك لمخاطر غسل الاموال وتمويل الارهاب.

9.1.2. عدم التسامح مطلقاً مع التسهيل المتعمد للجرائم المالية أو التحايل والانتهاكات للأنظمة والتعليمات والسياسات ذات العلاقة، وبالتالي ليس لدى البنك أية شهية لقبول جرائم غسل الأموال و/أو تمويل الارهابZero Tolerance for ML/TF risks

9.1.3. تجنب إجراء أية عمليات أو معاملات مالية لأفراد أو كيانات يعتقد أنها متورطة في سلوك غير مشروع أو غير قانوني

9.1.4. تجنب المخاطر التي يمكن أن تعرض الخطط الإستراتيجية للبنك للخطر، بما في ذلك الأنشطة التي يمكن أن تجعل البنك عرضة لأي نوع من الدعاوى العامة أو الخاصة، والتي قد تضر بسمعة البنك والتي تتسبب في سوء العلاقة مع الجهات الرقابية ذات العلاقة

9.1.5. تجنب أو تحجيم العمل مع أي شريحة من شرائح العملاء، والتي تعتقد الإدارة أن آليات الرقابة المتاحة بالبنك لا يمكنها حماية البنك من المخاطر التي لا يمكن قبولها.

9.1.6. يحتفظ البنك بحقه في رفض أو إنهاء علاقة العمل مع أي عميل، أو رفض قبول ايداعات، أو اجراء معاملات لا تتوافق مع سياسة البنك في قبول المخاطر

9.1.7. يقبل البنك فقط التعامل مع العملاء ذوي السمعة الطيبة الذين يستخدمون منتجاتهم وخدماتهم والحسابات ذات الصلة لأغراض مشروعة، ويمكن تحديد هوياتهم والتحقق منها ، ويتم فرض عناية واجبة معززة لكافة العمليات المالية للصرافين / الجمعيات والاشخاص المعرضين سياسيا للمخاطر .

9.2.سياسة قبول العملاء (العلاقات الممنوعة والمحظورة) : يلتزم البنك بعدم قبول أو التعامل مع أي من العملاء أو الأطراف الذين ينخرطون في أي من المحظورات التالية، وفي حال وجود علاقة قائمة مع البنك، يتم انهاؤها فوراً:

9.2.1. <u>الحسابات المجهولة:</u>

أ. لا يجوز للبنك انشاء علاقة أو فتح حساب أو التعامل مع أفراد/أشخاص/شركات و/أو أي هيئة و/أو مؤسسة مجهولة الهوية أو وهمية أو مشفرة بأسماء وهمية أو مستعارة أو باستخدام أرقام ورموز لاخفاء اسم أو هوية العميل، ويجب اخطار ضابط اتصال مكافحة غسل الاموال فوراً عن هذه الحالات.

ب. في حال كانت هناك مبررات مقبولة من البنك للحفاظ على سرية معلومات العميل، يجب الحصول على موافقة ضابط اتصال مكافحة غسل الاموال وتمويل الارهاب والمدير العام ، وأن يتم توقيع اتفاقية مع العميل بخصوص الحفاظ على سرية معلومات الحساب، شريطة خضوع الحساب للافصاح وفقاً للمتطلبات القانونية والتنظيمية، وأن يكون لضابط الاتصال حق الوصول الى البيانات والمعلومات الخاصة بالحساب.

9.2.2. **<u>المؤسسات الوهمية</u>**: لا يجوز للبنك إقامة علاقة أوالاحتفاظ بعلاقة عمل مع حسابات وهمية أو شركات أو بنوك أو أشخاص ليس لهم وجود فعلي، أو انشاء علاقة أو الاحتفاظ بعلاقة مع بنك مراسل في ولاية قضائية أجنبية يسمح باستخدام حساباته من قبل بنوك أو مؤسسات وهمية. وفي حال وجود أي

شك لدى دائرة مكافحة غسل الأموال وتمويل تمويل الإرهاب بهذا الخصوص، يجب التحقق من الوجود المادي وعدم وجود علاقة مع مؤسسات وهمية، بالطريقة المناسبة، قبل أو بعد انشاء علاقة العمل، ويتم ارسال تقرير اشتباه إلى وحدة المتابعة المالية في ذلك.

9.2.3. **الاشخاص المدرجين بقوائم الحظر:** لا يقبل البنك انشاء أو التعامل أو الاحتفاظ بعلاقة عمل مع عميل أو طرف مدرج بأي من قوائم الحظر أو العقوبات، أو يتصرف وكيلاً أو نيابة عن أو لمصلحة شخص أو طرف أو حكومة تخضع لعقوبات شاملة أو في حالة حظرها بموجب القانون أو اللوائح المعمول بها (على سبيل المثال لا الحصر قوائم OFAC، UN، EU ، القائمة المحلية للأمم المتحدة الصادرة عن لجنة تنفيذ قرارات مجلس الأمن في فلسطين وفق كتب سلطة النقد الفلسطينية)، ولا يستمر في التعامل معهم في حال تبين ادراجهم لاحقاً بعد فتح الحسابات.

9.2.4. الكيانات/ الدول الخاضعة للعقوبات:

أ. يمتنع البنك عن تقديم أي منتج أو التعاقد أو اجراء أية معاملة لصالح أفراد أو كيانات خاضعة للعقوبات، ويمتنع البنك عن الدخول في علاقة مع كيان أو فرد له صلة بالدول أو الكيانات الخاضعة للعقوبات، ويستعين في ذلك باحدى أدوات البحث الدولية مثل Know Your Country التي توفر البيانات والمعلومات لمعرفة وتقييم مخاطر البلدان، والبلدان الخاضعة للعقوبات وعالية المخاطر، كما يمكن الاستعانة بمؤشر بازل لمكافحة غسل الأموال الذي يستخدم في تصنيف مخاطر الدولة، وقائمة مجموعة العمل المالي "عالية المخاطر".

ب. لا يجوز فتح أي حسابات لأي بنوك و/أو مؤسسات مُدرجة ضمن قائمة الدول غير المتعاونة.

9.2.5. **التهرب الضريبي:** لا يقبل البنك ولا يتسامح مع التهرب الضريبي أو تسهيل أنشطة أو معاملات يمكن تفسيرها على أنها جريمة ضريبية، سواء من قبل شركائه أو موظفيه أو من ينوب عنه، أو الذين يساعدون أو يشجعون عن علم على التهرب الضريبي، ولا يشارك عن عمد في معاملات تسهل التهرب الضريبي.

9.2.6. **الانتهاك المتعمد للقانون والتعليمات وإساءة استخدام الحساب:**

أ. لا يقبل البنك التعامل مع الحسابات ذات الانتهاكات المتعمدة للقانون أو اللوائح أو السياسة المتعلقة بالجرائم المالية والاحتيال، وذات الانتهاكات المتكررة غير المقصودة أو العرضية للقانون أو اللوائح أو السياسة المتعلقة بالجرائم المالية و / أو الاحتيال

ب. لا يقبل البنك الحسابات التي يساء استخدامها في عمليات غسيل الأموال أو تمويل الإرهاب أو الاحتيال.

9.2.7. **الاحتيال والفساد:** لا يقبل البنك أي احتيال أو فساد أو أي مظهر من مظاهرهما، أياً كان مصدره، سواء كان من قبل العملاء أو موظفي البنك أو الأطراف الثالثة التي تعمل نيابة عن البنك. ويأخذ البنك جميع مزاعم الاحتيال أو الفساد المشتبه بها على محمل الجد، ويستجيب لها بشكل كامل ومنصف.

9.2.8. **رفض التعاون مع البنك:** لا يحتفظ البنك بحسابات ترفض تقديم المعلومات أو الوثائق الكافية التي يطلبها.

9.2.9. **الحسابات من خلال وكيل أو وسيط:** لا يقبل البنك الحسابات التي تفتح من قبل وكيل أو وسيط مالي وباسمه هو لمجموعة من العملاء دون اظهار اسماء أي منهم)، والتعامل بالحساب لصالح هذه المجموعة دون معرفة البنك بهم أو التواصل معهم (اخفاء المستفيدين الحقيقيين).

9.2.10. **استغلال علاقات المراسلة:** لا يقبل البنك اقامة علاقةعمل ينتج عنها استغلال لعلاقة المراسلة الخاصة به للوصول الى النظام المالي الذي يتعامل معه البنك أو اجراء معاملات من خلاله.

9.2.11. **فتح الحسابات دون حضور شخصي:** لا يجوز فتح حسابات بالمراسلة لأشخاص غير مقيمين دون التعرف على هويتهم وشخصياتهم الأصلية بالوسائل المناسبة.

9.2.12. **العملاء الممتنعين ذوي المؤشرات الامريكية:** لا يتم فتح حسابات للعملاء الذين تتوفر لديهم مؤشرات بأنهم أمريكان ويرفضون التوقيع على النماذج المخصصة لذلك.

9.2.13. الحسابات المرتبطة بجرائم:

أ. لا يقبل البنك الحسابات المتعلقة بجرائم مثل (صنع الاسلحة والذخائر والاتجار بها بصورة غير مشروعة ، الاتجار بالبشر ، المواد الاباحية وغيرها .

اذا لم يستطع البنك الوفاء بالتزاماته بشأن بذل العناية المتواصلة المذكورة في السياسة ، فليس له أن يقيم علاقة عمل أو يستمر فيها وضرورة رفع تقرير اشتباه لوحدة المتابعة المالية.

9.2.14. نقاط البيع (POS): في حال كان العميل مرتفع المخاطر فان فتح الحساب يتطلب موافقة مسبقة من دائرة غسل الاموال بعد ارفاق المستندات المعززة (النشاط والدخل ، توقيع الاستبيان الخاص بقاعدة KYC) ويتم تحديد تاريخ تحديث البيانات القادم بناء على مخاطر العميل ، وفي حال كان العميل مرتفع المخاطر ، فان ذلك يتطلب موافقة مسبقة من دائرة مكافحة غسل الاموال بعد التحقق من المستندات المطلوبة وتتم هذه العملية بشكل آلي .

10. تنفيذ قرارات مجلس الامن :

10.1. يتوجب على المؤسسات المالية وخلال (24) ساعة من نشر قائمة الامم المتحدة او قائمة الادراج الوطنية على الموقع الالكتروني للجنة اتخاذ الاجراءات اللازمة للاستعلام والاضافة وتجميد الاصول في حال وجودها وتوثيق ذلك ، والرد للجنة تنفيذ قرارات مجلس الامن بما تم اتخاذه ، وكذلك الحال في حال الحذف من القوائم (مادة 13) .

10.2. تلتزم البنوك بعدم اتاحة اي اموال او اصول اخرى او موارد اقتصادية او تقديم خدمات مالية للاشخاص المدرجين على القوائم بشكل مباشر او غير مباشر ، او لاي شخص او كيان يتصرف نيابة عنه او بتوجيه منه بدون تخويل او اذن او اشعار بموجب قرارات مجلس الامن ذات الصلة (مادة 14).

10.3. يعتبر نشر / حذف الاسماء المدرجة على قائمة الامم المتحدة وقائمة الادراج الوطنية على الموقع الالكتروني للجنة بمثابة اخطار كافي للاشخاص والكيانات المدرجين و / أو الذين حذفت اسماؤهم المدرجة وفقا للقوانين واللوائح المعمول بها (مادة 20) .

10.4. يتوجب الاحتفاظ بالسجلات حول الحسابات والمعاملات العائدة للشخص / الكيان المدرج طوال فترة ادراجه ولمدة (10) سنوات على الاقل بعد حذف الاسم المدرج وفق احكام القانون (مادة 23).

10.5. يتوجب تزويد اللجنة بالمعلومات المرتبطة بتنفيذ احكام القانون عند الطلب مع حصر استخدام هذه المعلومات للهدف الذي تم الحصول عليها لأجله .

10.6. يتوجب تزويد اللجنة بالمعلومات اللازمة حول وضـع الاموال والاصـول المجمدة او التي تم رفع التجميد عنها واي اجراءات اخرى تم اتخاذها بشأنها .

تاسعاً: الابلاغ عن العمليات المشبوهة

1. **الابلاغ داخليا عن الانشطة والمعاملات المشبوهة:**

يتوجب على جميع الموظفين المعنيين كلا بحسب موقعه عند اكتشاف أي حالة مثارا للشك و/أو في حال الاشتباه بأي حساب أو عملية مصرفية تعبئة نموذج اشتباه المعد من قبل سلطة النقد الفلسطينية ورفعه لوحدة مكافحة غسل الاموال وتمويل الارهاب في الإدارة العامة لاتخاذ الإجراءات اللازمة مع ضرورة الالتزام بما يلي للاهمية:

1.1. يتوجب عدم اعلام العميل عن نية البنك رفع تقرير اشتباه به او تحذيره.

1.2. في حال الشك بقوة بوجود نشاط غير قانوني بحركة معينة، يتوجب عدم استكمال التنفيذ، ويجوز استكمال التنفيذ في حال تعرضك او أحد الموظفين لخطر حقيقي بسبب عدم التنفيذ.

1.3. يتوجب تقديم تقرير حركات مشبوهة حتى في حال عدم اكتمال التنفيذ، وعلى سبيل المثال في حال تقديم العميل لهوية من الواضح انها مزورة.

1.4. لتعبئة تقرير حركات مشبوهة حسب الاصول، يتوجب الحصول على (اسم العميل / عنوانه / رقم الهاتف / تاريخ الميلاد / معلومات اثبات الشخصية / مكان الاصدار.

1.5. يتوجب تعبئة تقرير الحركات المشبوهة مباشرة بعد مغادرة العميل والاحتفاظ بنسخة منه مع المستندات المعززة لفترة لا تقل عن خمس سنوات وحسب التعليمات.

2. **الابلاغ خارجيا لوحدة المتابعة المالية**

في حال ثبوت الشك / الاشتباه، يتم إغلاق حساب العميل وانهاء غلاقة العمل معه وابلاغ وحدة المتابعة المالية بذلك.

3. **اعتبارات ما بعد تقرير الاشتباه:** ان تقديم تقرير اشتباه لا يعفي البنك من الاستمرار في إتخاذ إجراءات العناية الواجبة بشأن علاقة العمل مع العميل.

عاشراً: بذل العناية الواجبة:

1. **العناية الواجبة** : تعرف العناية الواجبة CDD بأنها مجموعة الاجراءات التي يجب أن يقوم بها البنك، لتحقيق التزامه بجميع القوانين واللوائح ذات الصلة وممارسات العمل السليمة، مما يقلل من احتمالات وقوعه ضحية لأنشطة غير قانونية من قبل عملائه وتساعد في فهم وتقييم العميل والتعرف عليه وعلى مخاطره المحتملة، وهل هناك اشتباه أو شك في نشاطه أم لا، ومن ثم التقرير فيما اذا كان سيتم انشاء علاقة عمل معه من عدمه، ويجب أن لا ينشئ البنك علاقة عمل، مع العملاء الذين لا يستوفون الحد الأدنى من معايير القبول الموضحة في هذه السياسة ووفقاً لدرجة مخاطرهم ، بحيث يتم التاكد بدرجة معقولة مما يلي :

1.1. تحديد هوية العميل والتحقق منها، من خلال المعلومات والبيانات والمستندات الأصلية.

1.2. التحقق ما إذا كان العميل يتصرف نيابة عن شخص آخر صاحب المصلحة الحقيقية من الحساب أو المعاملة.
1.3. فهم ملف تعريف العميل، وأعماله ونشاطه وحركة حسابه.
1.4. فهم الغرض والسبب من إقامة علاقة مع البنك، ومستوى وحجم النشاط.
1.5. فهم مصدر ثروة العميل وأمواله.
1.6. معرفة المعلومات السلبية ذات الصلة.
1.7. تقييم مخاطر احتمال الانخراط في انشطة غسل الأموال و/أو تمويل الإرهاب، والمساهمة في دعم اتخاذ القرارات القابلة للتنفيذ للتخفيف من المخاطر الختلفة.

2. **مستويات العناية الواجبة:** يختلف مستوى العناية الواجب بذله تجاه العملاء المحتملين والحاليين، وفقاً لدرجة مخاطرتهم وأنماطهم، وطبيعة نشاطاتهم وتعاملاتهم، على النحو التالي:

2.1. تطبق تدابير العناية الواجبة المبسطة (SDD)، لتحديد الهوية والتعرف على العميل، للعملاء منخفضي المخاطر بحيث يطلب أقل قدر ممكن من المعلومات والبيانات واجراءات التحقق من العميل.
2.2. تطبق تدابير المستوى القياسي من العناية الواجبة (CDD)، تجاه العملاء غير مرتفعي المخاطر ويعتبرون متوسطي المخاطر، من خلال اجراءات تعتبر وسطاً بين العناية الواجبة والمتوسطة والعناية الواجبة المشددة أو المعززة EDD.
2.3. تطبق العناية الواجبة المعززة (EDD)، تجاه العملاء مرتفعي المخاطر حيث تطلب معلومات وبيانات ومستندات وحيث تطبق معايير وتدابير أكثر تشدداً تجاههم.
2.4. تطبق اجراءات العناية المتواصلة قبل او اثناء علاقة العمل او عند تنفيذ عمليات للعملاء العارضين .

3. **تحديد هوية العميل والتحقق منها وتوقيتها :**

قبل أو أثناء علاقة العمل ، يجب تحديد هوية جميع العملاء والأطراف ذوي الصلة بما في ذلك المستفيد الحقيقي في حالة الشخصيات الاعتبارية، وأي شخص آخر يتصرف نيابة عن العميل مثل المفوضين بالتوقيع والوكلاء عن العميل، الذين يعتزم البنك التعامل معهم بناءً على المعلومات المقدمة منهم والمصادر العامة المتاحة حولهم والتحقق من صحة المعلومات التي تم الحصول عليها من أجل فهم المستوى الأساسي للمخاطر وتحديد فئة مخاطر العميل وتقع المسؤولية في ذلك على خط الدفاع الأول أي الموظفين المكلفين بالتعامل مع العميل وتنفيذ طلبه ، حيث يجب عليهم التأكد أن الاثباتات التي تم الحصول عليها كافية بشكل معقول للتحقق من هوية وشخص العميل وفي حالة عدم تمكنهم من الحصول على أدلة كافية أو الشك في مدى كفايتها عليهم الرجوع الى ضابط اتصال مكافحة غسل الاموال وتمويل الارهاب بالبنك الذي سوف يدرس الوضع وفقاً لهذه السياسة واجراءات اعرف عميلك وإذا لم يقدم العميل دليلًا على الهوية بطريقة تسمح للبنك بالامتثال لمتطلبات هذه السياسة وأية تعليمات ذات علاقة ولم يتمكن البنك من الحصول على المعلومات والوثائق الكافية يجب التوقف عن تنفيذ النشاط / الخدمة لهذا العميل أو إنهاء أي تفاهم سابق تم التوصل إليه مع العميل ، وتشمل اجراءات التعرف للشخصيات الاعتبارية ، هيكل الملكية والسيطرة الخاص بالعميل وتحديد الشخص أو الأشخاص الطبيعيين الذين يمتلكون أو يسيطرون على العميل ، عندما يكون الكيان القانوني عبارة عن شراكة أو جمعية، يجب الحصول على هوية جميع الشركاء / المديرين والتحقق منها.

أهداف التعرف على هوية العميل:

- منع العملاء ذوي النوايا الإجرامية من استخدام البنك للقيام بأنشطة ذات علاقة بغسل الأموال والجرائم المالية.
- تمكين االبنك من معرفة وفهم وتتبع العمليات المالية التي يقوم بها العملاء بشكل أفضل وذلك لتجنب البنك أية مخاطر محتملة نتيجة ذلك.
- وضع الإجراءات والضوابط الرقابية للحد من العمليات المشبوهة وتوفير آلية تقارير عنها داخل البنك تمشيا مع الإجراءات المعمول بها فيه.
- التوافق مع القوانين والأنظمة والتشريعات والسياسات سواء الصادرة عن الجهات الرقابية (المحلية والدولية) أو الداخلية الصادرة عن البنك.
- اتخاذ الإجراءات والخطوات اللازمة للتأكد أن كافة موظفي البنك تم تدربهم للتعرف على إجراءات وقواعد اعرف عميلك وعمليات غسل الأموال.

4. **تاجيل متطلبات التعرف على اجراءات العناية الواجبة : وبالرغم من أنه لا يجوز السماح بانشاء العلاقة، الا أنه يجوز تأجيل اجراءات التحقق من الهوية** وفق ما اجازته تعليمات اللجنة الوطنية رقم 2016/2 إلى ما بعد المباشرة في علاقة العمل، وذلك وفقاً للشروط التالية مجتمعة:
   - استكمال إجراءات التحقق في أقرب وقت ممكن.
   - أن يكون التأجيل ضرورياً لإنجاز مهام العمل العادية، بحيث لا يترتب على ذلك أيّة مخاطر غسل الأموال أو تمويل الإرهاب .
   - دراسة مخاطر غسل الأموال وتمويل الإرهاب للحالة التي تّم التأجيل فيها، والسيطرة على تلك المخاطر.
   - أن تتوفر لدى الشركة إجراءات معتمدة وواضحة بالخصوص.
   - أن تكون مخاطر غسل الأموال وتمويل الإرهاب منخفضة وتتم إدارتها بفعالية.
   - أن يكون قد تم فحص أسماء جميع الأطراف ذوي العلاقة، وأن يكون قد تم حل أية مشكلة نتيجة هذا الفحص.
   - ألا تتجاوز قيمة المعاملة المالية التي يرغب العميل باجراءها عن مبلغ 5000 دولار أمريكي.
   - أن يتم استيفاء النواقص على وجه السرعة خلال فترة لا تتجاوز خمسة عشر (15) يوم عمل من تاريخ التأجيل.

وعندما يؤجل إتمام اجراءات العناية الواجبة بشأن العميل، يجب أن تحدد بوضوح أسباب ومدى ضرورة التأجيل وأن تؤكد استيفاء جميع الشروط المذكورة أعلاه. وأن يوقع على ذلك الموظف المسؤول عن اجراءات المباشرة في علاقة العمل، والمدير المباشر ذي الصلة.

في حالة انتهاء فترة التمديد التي تبلغ 15 يومًا دون استكمال اجراءات التحقق من الهوية، يجب عدم المضي قدمًا في العلاقة ويجب إنهاء هذه العلاقة.

5. **الفحص على القوائم:**

يجب فحص اسم العميل وجميع الاطراف ذوي الصلة به من خلال نظام القوائم السوداء، ومن ثم تحديد قبول انشاء العلاقة أو رفضها منذ البداية وفي حال وجود تطابق أو شك في التطابق يجب عدم القيام بأي عمل مع العميل أو نيابة عنه حتى يتم التحقق من عدم وجود شبهة أو أن التطابق غير صحيح، أما اذا ثبتت صحة التطابق، فانه يتم رفض انشاء العلاقة، وانهاء العلاقة القائمة في حال وجودها ويجب الاحتفاظ بسجل نتائج الفحوصات لأغراض المراجعات اللاحقة للعميل.

يجب الحصول على اسم العميل باللغة الانجليزية لغايات الفحص بنظام القوائم السوداء، والانتباه لطريقة وأحرف كتابة الاسماء، ويمكن الاعتماد في ذلك على المستندات المختلفة التي يتم الحصول عليها من العميل والتي قد تظهر التهجئة المختلفة أو لأحرف كتابة الاسم باللغة الانجليزية، وكذلك مختصرات الاسم وأية اشكال يتم التعبير فيها عن الاسم بحيث يتم فحصها جميعاً مع التأكيد على ما يلي :

5.1. التزام البنك بالفحص على القوائم المحلية (قائمة البنك الداخلية) والدولية (ofac, un , eu , French) المحدثة عند فتح حساب جديد لعميل.

5.2. فحص كافة عملاء البنك على القوائم السوداء مرتين سنويا على الاقل وتوثيق النتائج .

6. الحصول على معلومات اضافية للتعرف على العميل:

لتقييم مخاطر العميل بشكل أفضل، ولغايات التعرف على هوية العميل وأنشطته، يتم الحصول على المزيد من المعلومات والتي تشمل:

6.1. الغاية من إقامة العلاقة:

يجب الحصول على اجابة واضحة وموثقة حول الغاية من انشاء العلاقة، وتفاصيل الخدمات التي يطلبها أو يرغب بالحصول عليها وسبب أو أسباب ذلك، ومدى تناسبها مع نشاطه.

6.2. مستوى وحجم التعامل المتوقع:

يجب الحصول على هذه المعلومات ويستفاد منها في التحقق من مدى تناسبها لاحقاً مع النشاط والتعامل الفعلي للعميل. يجب الحصول على تقدير معقول لحجم المعاملات المتوقع القيام بها سواء شهرياً أو سنوياً أو لأي فترة، بحيث يمكن الاستناد اليها عند مراقبة وتقييم حركة حساب العميل.

6.3. المعاملات الخارجية:

معرفة ما اذا كان العميل يعتزم أو ينوي أو أن له فعلياً علاقات أو تعاملات خارج البلاد، والتحقق أنها ليست دول او مناطق مرتفعة المخاطر أو محظورة.

6.4. مصدر الدخل source of income:

من المهم معرفة مصدر الدخل وأية مصادر أخرى أو اضافية للدخل التي سوف ترد للحساب.

6.5. مصدر الأموال source of funds:

هناك علاقة وارتباط وثيق بين مصدر الاموال وكلا من الغاية من انشاء العلاقة وطبيعة النشاط الذي يفترض أنه مصدر الاموال التي ترد للحساب، لذلك يجب التحقق أن الأموال المحولة أو الواردة للحساب تأتي من نشاط أو عمل العميل، وبذل العناية الواجب المعززة خاصة في حال الأشخاص مرتفعي المخاطر وفي حال ورود أموال من طرف ثالث، فيتم الحصول على مزيد من المستندات والوثائق المعززة مثل إثبات الملكية للطرف الثالث، الفواتير المتعلقة بالمعاملات الخاصة بالعميل.

6.6. مصدر الثروة source of wealth:

أهمية هذه المعلومات أنها يمكن أن تفيد في تفهم مصادر الاموال المتجمعة (الثروة) خلال فترة زمنية معينة، والنظر في مدى كونها مناسبة ومعقولة لطبيعة العلاقة مع الشركة، في حال صعوبة أو عدم توفر إثبات لهذه المعلومات، يجب على الموظفين ذوي العلاقة الاحتكام للتقدير الجيد والخبرة والتسجيل الدقيق والكامل والتقييم المعقول لمدى معقولية المعلومات التي تم جمعها.

6.7.طبيعة العمل أو النشاط nature of business or activity:

من المهم معرفة طبيعة عمل أو نشاط العميل، حيث أنه سيتم ربط طبيعة العمل أو النشاط مع مصادر أموال العميل كمصـــدر الدخل أو الثروة والاموال الواردة للحســـاب، ويجب توثيق كيفية قيام العميل بجني الأموال التي ســـيتلقاها البنك، مما يتطلب معرفة طبيعة عمل العميل أو نشاطه ويمكن الحصول على معلومات مهمة عن العميل من خلال المصادر العامة للمعلومات، مثل خضوع العميل لإجراءات رقابية أو تنظيمية، الكشف عن تحقيقات جارية أو دعاوى متعلقة بمكافحة غسـل الأموال أو تمويل الإرهاب، عقوبات، جرائم أخرى خطيرة، أو قضـايا مرفوعة في المحاكم وإذا تم العثور على أي معلومات سلبية، يجب تسجيل النتيجة في سجل العناية الواجبة للعميل، وإبلاغ ضابط الاتصال للنظر في الإجراءات والضوابط المناسبة التي يجب وضعها.

7. ربط مستوى العناية الواجبة المطلوب بدرجة مخاطرة العميل :

يساعد تقييم وتحديد درجة مخاطرة العميل وتصنيفه بهذا الخصوص، في تحديد مستوى العناية الواجبة المطلوب للعميل، والذي يتم على مرحلتين:

الاولى: تحديد المخاطر الأولية للعميل عند انشـــاء العلاقة، بناء على المعلومات المتاحة في حينه وفق متطلبات تدابير اعرف عميلك وبذل العناية الواجبة.

الثانية: بعد انشـاء العلاقة، وفق معاملات العميل وأنماط عملياته وحركة حسـابه، من خلال مراقبة تعاملاته ونشـاطه، الى جانب معلومات اعرف عميلك وبذل العناية الواجبة، ومن ثم تحديد درجة مخاطرة العميل الكلية التي تعكس جميع ما قد يكون عرضة لمخاطر غسل الاموال وتمويل الارهاب المتعلقة به.

8. العناية الواجبة المبسطة SDD

تطبق اجراءات وتدابير العناية الواجبة المبسـطة وفق تعليمات اللجنة الوطنية رقم 2016/2 للعملاء منخفضـي المخاطر، ولا تطبق في حال المعرفة أو الشـك أو الاشـتباه أن العميل منخرط بغسـل الاموال أو تمويل الارهاب، أو أن المعاملة تتم نيابة عن شـــخص آخر منخرط في أنشـــطة غســـل الاموال أوالارهاب، أو أن الهدف من المعاملة خرق أو تجاوز القيود المفروضة بموجب التعليمات. كما لا تطبق للعملاء مرتفعي المخاطر.

يجب قبل تطبيق تدابير العناية الواجبة المبسطة، التحقق وفق الوثائق والمستندات التي يجب توفرها لدعم تصنيف العميل باعتباره منخفض المخاطر والتحقق أنه يقع في فئة العملاء منخفضـي المخاطر وذلك قبل فتح الحسـاب أو انشـاء العلاقة وتطبق تدابير العناية المبسطة على الاشخاص الاعتباريين، ولا يلزم الحصول على الأدلة مباشرة من العميل ، حيث يمكن التحقق المسـتقل المقبول من هوية العميل من خلال نسـخة أو تقرير منشـور بموقع الجهة الرقابية أو التنظيمية، أو تقرير منشور بموقع بورصـة فلسطين، أو قرار أو وثيقة حكومية أو بموجب تشريع قانوني، أو تأكيد طرف ثالث موثوق معروف جيدًا حيثما كان ذلك متاحًا.

ومن أمثلة الأشخاص الاعبتاريين الذين تطبق معهم تدابير العناية المبسطة:

- الوزارات والهيئات والشركات الحكومية وشبه الحكومية.
- الشركات المدرجة في سوق الأوراق المالية الخاضـعة لمتطلبات الإشراف والرقابة والإفصـاح المفروضـة على الشركات العامة وفقًا لمعايير الإفصاح المقبولة دوليًا.
- الشركات ذات السمعة الطيبة والمعروفة، مثل الشركات الخاصة العريقة ذات الأنشطة الموثقة التي تعمل فيها ومصادر تمويلها معروفة بالإضافة إلى المعرفة الجيدة لأصحاب المؤسسة والمراقبين فيها.

9. العناية الواجبة المعززة EDD

يتعين اتخاذ تدابير العناية الواجبة المعززة EDD في الحالات التي تكون مطلوبة بموجب القانون أو التعليمات ذات العلاقة، والعملاء مرتفعي المخاطر، وتتضمن المتطلبات التالية:

- إجراء تحقق إضافي من هوية العميل.
- التحقق من مصدر الثروة ومصدر الاموال.
- التأكد أن مصدر المعاملة الأولى (إذا لم تكن إيداع نقدي) هو من حساب مصرفي باسم العميل في بنك يخضع لمعايير سلطة النقد الفلسطينية أو جهة رقابية مناظرة.
- فحص المعلومات العامة والسلبية للعميل.
- المراقبة المستمرة " يتوجب بذل المزيد من العناية والمراقبة المستمرة لتعاملات العميل .
- موافقة أو توصية ضابط الاتصال / موافقة الادارة العليا : الحصول على الموافقات اللازمة لانشاء العلاقة و / أو الاستمرار بعلاقة العمل مع العميل .

10. العناية الواجبة للموردين ومزودي الخدمات:

كقاعدة عامة، لا يجوز إقامة علاقة عمل قبل تطبيق اجراءات العناية الواجبة المناسبة تجاه المورد أو المزود للخدمة، وتحديد هويته وفحص الشركات أو المؤسسات والقائمين عليها من خلال نظام القوائم السوداء كجزء من تدابير العناية الواجبة للمشتريات والحصول على الخدمات مادية أو استشارية، وقبل انشاء علاقة العمل وفقاً لمتطلبات هذه السياسة، والحصول على جميع الوثائق اللازمة بما في ذلك وثائق اثبات الشخصة وشهادات التسجيل ومراجعتها من قبل ضابط الاتصال بالبنك لتطبيق مستوى العناية الواجبة المناسب. ويجب رفض انشاء علاقة مع مورد أو مزود خدمة لا يتوافق مع متطلبات هذه السياسة.

- يجب أن يحتفظ البنك بالسجلات والمستندات والوثائق اللازمة لتقديمها للجهات التدقيقية أو الرقابية أو التنظيمية المخولة سواء داخل البنك أو خارجه في حال طلبها.

11. **العملاء مرتفعي المخاطر** : تُطبق اجراءات العناية الواجبة بصفة خاصة بغض النظر عن نتيجة تقييم مخاطرة العميل على الفئات التالية من العملاء باعتبارها عالية المخاطر بشكل افتراضي:

11.1. غير المقيمين

يجب فرض ضوابط كافية للتحقق من هوية العملاء غير المقيمين والمصادقة عليها، وتطبيق كافة متطلبات العناية الواجبة المعززة وفق إجراءات اعرف عميلك.

11.2. الصرافين

تعتبر شركات ومحلات الصرف مرتفعة المخاطر بالرغم من ترخيصها من سلطة النقد، حيث أنها تتعامل مع عملاء عابرين وغير مستمرين ولا تحتفظ بعلاقة موثقة مع العملاء الا لعدد قليل جداً من العملاء، وتطبق الحد الأدنى من متطلبات التعريف لاجراء المعاملة، مع اجراء العديد من عمليات الصرف وتبديل العملات وبشكل متكرر جداً، و لذلك يجب أن تخضع عملية فتح حساب أو انشاء علاقة عمل مع هذه الشركات لاجراءات العناية الواجبة المعززة والحصول على موافقة الدوائر ذات العلاقة والمدير العام وتخضع للرقابة المستمرة.

11.3. المعرضون سياسيًا PEPs

وهم الاشـخاص الطبيعيين سـواء كانوا مواطنين فلسـطينيين أو أجانب وذوي الصـلة بهم وفق تعريف المعرضـين سـياسـياً بموجب تعليمات الجهات الرقابية ذات العلاقة، وكما هو مبين في هذه السـياسـة والأشـخاص المعروفين بأنهم شـركاء مقربون من هؤلاء الأشـخاص مثل المديرون والمفوضـين بالتوقيع عنهم ... إلخ، كونهم معرضـون للفسـاد المالي والاداري بشـكل كبير بسـبب تمتعهم بامكانات واسـعة للسـيطرة والوصـول للأموال العامة واسـاءة استتخدام النفوذ.

- ✓ يجب أن يخضـع هؤلاء العملاء للمراجعة الصـارمة والمسـتمرة واجراءات العناية الواجبة واعرف عميلك، كما يجب الحصول على نائب المدير العام عند انشاء العلاقة.
- ✓ يجب الاحتفاظ بقائمة داخلية للأشـخاص السـياسـيين للتحقق من بيانات "اعرف عميلك"، وفحص المعلومات العامة حول شخصيتهم وفي حال اكتشاف أن عميل قائم أو أنه أصبح لاحقاً معرض سياسياً، يجب مراجعة معلوماته وتطبيق متطلبات العناية الواجبة المعززة .
- ✓ يجب على الأشـخاص من هذه الفئة أن يقوموا بتعبئة نموذج ملحق فتح الحسـاب الخاص بمراقبة الامتثال والذي يتضمن المزيد من البيانات والمعلومات ومنها:
  - طبيعة نشاط مالك الحساب.
  - مصادر الدخل والأموال.
  - الغرض من فتح الحساب (حجم التداول، ومدة التداول، تحديد الأسواق أو الشركات المدرجة.....)
  - العمليات المستقبلية المتوقعة على الحساب
  - بيانات المفوضين أو الوكيل
  - سبب التصنيف كشخص ذو مركز سياسي
  - المستفيد الحقيقي من الحساب وبياناته
- ✓ يجب على الشـركة اتخاذ إجراءات كافية للتأكد من مصـادر ثروة العملاء والمسـتفيدين الحقيقيين الذين يندرجون ضمن هذه الفئة.
- ✓ يجب على الشركة أن تتابع بشكل دقيق ومستمر تعاملاتها مع هؤلاء العملاء.

11.4. الجمعيات الخيرية والهيئات والشركات غير الربحية:

تعتبر هذه الكيانات مرتفعة المخاطر كونها منظمات تعمل بشكل رئيسـي في مجال جمع أو توزيع الأموال، ضـمن برامج وأنشـطة تركز على الخدمات الاجتماعية والتعليم والرعاية الصـحية والانشـطة الخيرية والدينية والثقافية وغيرها، وأن آلية جمع الاموال وصـرفها للأغراض المختلفة عرضـة بشكل كبير لسوء الاستخدام، مثل الاستخدام في غسل الأموال أو تمويل الإرهاب، هذا بالاضـافة الى ضـعف الضـوابط الرقابية على هذه الانشطة، مما يعرض البنك لمخاطر السـمعة اضـافة للمخاطر المالية و/أو القانونية ، وتطبق إجراءات العناية الواجبة المعززة EDD في حال توفر أي من المؤشرات التالية:

- أن تكون فرعاً لمنظمة أجنبية مقرها الرئيسـي في دولة مرتفعة المخاطر أو دولة تحت المتابعة المعززة ضـمن القوائم الصادرة عن وحدة المتابعة المالية و/ أو لديها فروع في تلك الدول.

- لها علاقة/ علاقات عمل مع الدول مرتفعة المخاطر أو الدول تحت المتابعة المعززة أو الدول تحت اجراء مراقبة مستوى التقدم في الالتزام بمعايير مجموعة العمل المالي
- حجم ايراداتها السنوية يزيد عن 100,000 دولار أمريكي، ونشاطها الرئيسي يندرج ضمن الانشطة الخدماتية.
- سبق رفع تقرير اشتباه بها لوحدة المتابعة، او ورود استفسار او طلب معلومات عنها من جهات الاختصاص.

11.5. العملاء ذوي المخاطر المرتفعة بالنسبة لعمليات غسل الأموال وتمويل الإرهاب.

11.6. يجب على البنك تصنيف كافة عملائه حسب درجة المخاطر المتعلقة بغسل الأموال وتمويل الإرهاب مع مراعاة ما يلي:

- مدى تناسب عمليات وحركة الحساب التي يجريها العميل مع طبيعة نشاطه.
- مدى تشعب الحسابات المفتوحة لدى البنك والتداخل فيما بينها ودرجة نشاطها.

11.7. العملاء الذين ينتمون لدول مرتفعةالمخاطر او تحت العناية المعززة : في حال كانت هناك معاملات لعملاء ينتمون لدول لا تتوافر لديها نظم مناسبة لمكافحة غسل الأموال وتمويل الارهاب، يولي البنك عناية خاصة لمثل هذه العمليات ويتم فحصها بدقة بحيث اذا تبين أن العملية / العمليات لا تستند الى مبررات اقتصادية واضحة ولم يتمكن البنك من الوقوف على الظروف المحيطة بهذه العمليات وأغراضها فانه يتم التحفظ عليها ويمتنع البنك عن تنفيذ مثل هذه العمليات.

11.8. حسابات الهيئات الأجنبية والمستشارين الأجانب:

يجب على دائرة مكافحة غسل الأموال في البنك التأكد أن نشاط حسابات الهيئات الأجنبية يتناسب مع الغرض منها وطبيعة نشاط الهيئة وعدم وجود أية حركات غريبة على الحساب تتنافى مع الغرض من فتح الحساب.

11.9. تحديث البيانات : يتوجب تحديث بيانات العملاء وفق النهج القائم على المخاطر وحسب التعليمات والقوانين النافذه.

12. **المستفيد الحقيقي بالنسبة للشخص الطبيعي :** يتوجب على المؤسسات المالية وفقا لمخاطر غسل الاموال وتمويل الارهاب التي تنشأ عن العميل وعلاقة العمل تحديد المستفيد الحقيقي والتأكد من هويته من خلال تحديد ما اذا كان العميل يتصرف بالاصالة عن نفسه ولمصلحته وتوقيعه بما يفيد ذلك ، وبخلاف ذلك او وجود شكوك لدى البنك حول صحة اقرار وتصريح العميل ، تحديد الصفة التي يتصرف فيها العميل نيابة عن المستفيد الحقيقي وتطبيق اجراءات التعرف والتحقق على المستفيد الحقيقي وبما يقنع البنك بأنه تعرف على المستفيد الحقيقي من الحساب ، وكذلك الحال بالنسبة للشخص الاعتباري .

13. الاخفاق في إستكمال اجراءات العناية الواجبة : يتوجب على المؤسسات المالية في حال تعذر الالتزام باجراءات العناية الواجبة تجاه العملاء :

1. **عدم فتح الحساب او بدء علاقة العمل او تنفيذ عمليات .**
2. **انهاء علاقة العمل بالنسبة العملاء الحاليين .**
3. **النظر في رفع حالة اشتباه لوحدة المتابعة بشأن العمليات او الانشطة المشبوهة للعميل .**

14. الاعفاء من مواصلة اجراءات العناية الواجبة : يجوز للمؤسسة المالية عدم مواصلة تطبيق اجراءات العناية الواجبة في الحالات التي يتوفر فيها مؤشرات اشتباه بغسل اموال او تمويل ارهاب اذا كان من شأنها تنبيه العميل بهذا الاشتباه بناء على اسباب منطقية تيتم توضيحها في تقرير يقدم للوحدة بشكل فوري حول العملية او النشاط المشبوه .

15. **علاقات المراسلة** : يتوجب على المؤسسات المالية اتخاذ الاجراءات التالية حيال علاقات المراسلة المصرفية التي تتم عبر الحدود :

1. جمع معلومات كافية عن المؤسسة لفهم كامل لطبيعة عملها .
2. استخدام المعلومات المنشورة للتعرف على سمعة المؤسسة ومستوى الرقابة التي تخضع لها ، والتحقق من عدم خضوعها لتحقيق متعلق بقصور في ضوابط واجراءات غسل الاموال .
3. تقييم ضوابط واجراءات غسل الاموال وتمويل الارهاب .
4. الحصول على موافقة الادارة العليا قبل البدء بعلاقة مراسلة جديدة .
5. عدم الدخول في علاقة مراسلة مع بنوك صورية او الاستمرار فيها ، وكذلك التاكد من ان المؤسسة المصرفية المتلقية لا تسمح باستخدام حساباتها من قبل بنوك صورية

16. **اعرف موظفك Know Your Employee :**

يعد تطبيق مبدأ اعرف موظفك من أهم الامور التي يجب أخذها بالاعتبار نظراً للمخاطر التي يمكن أن تنشأ من خلال الموظفين ، وذلك نظراً لقدرة الموظف على الوصول الى المعلومات خاصة ذات الأهمية وحساسيتها والصلاحيات الممنوحة له، ومخاطر الانخراط في قضايا غسل الاموال بما يشمل الرشوة والغش والتزوير واستغلال المنصب الوظيفي وتسهيل معاملات مشبوهة وغيرها ، وتطبيق تدابير اعرف موظفك على مستويين:

- قبل أو عند التعيين:

يجب الاهتمام بحسن اختيار الموظفين ودراسة سيرتهم الوظيفية، والتحقق من عدم ادراج المرشح للعمل بالشركة على أي من قوائم الحظر المعتمدة.

- الموظفين القائمين على رأس عملهم:

يتم إعادة التحقق من الاجراءات المتخذة عند أو قبل التعيين، ومراقبة سلوكياتهم التي قد تعتبر مؤشرًا على تورط الموظف في عمليات غسل أألموال وتمويل الارهاب، مثل:

- ارتفاع مستوى معيشة الموظف ومستوى أنفاقه بشكل ملحوظ بما لا يتناسب مع دخله الشهري.
- تفادي قيام الموظف بأي إجازات.
- قيام الموظف بتجاوز الاجراءات الرقابية بشكل متكرر واتباع سياسة المراوغة خلال أدائه لعمله .
- قيام الموظف بالمساعدة في تنفيذ عمليات تتميز بأن المستفيد النهائي أو الطرف المقابل غير معروف فيها بشكل كامل .
- قيام الموظف بالمبالغة في مصداقية وأخلاقيات وقدرة ومصادر العميل المالية وذلك ضمن تقاريره بالخصوص.

حادي عشر: الاحتيال:

تشمل مخاطر الاحتيال والاختلاس والتزوير كافة قطاعات الاعمال ولا تقتصر على مؤسسة بعينها في القطاع الخاص سواءً كانت المؤسسة مالية أو صناعية أو خدماتية، اضافة الى أن التلاعب / الاحتيال / الاختلاس / التزوير يتكيف مع المتغيرات التي قد تطرأ على أي قطاع، ويستمر بالرغم من آليات التدقيق الداخلي والمراقبة والتقصي وشروط مراجعي الحسابات الخارجيين المستقلين وقواعد السلوك المهني.

يحدث الاحتيال على العملاء عندما يقنع المجرمون العملاء او يخدعونهم لتحويل اموال الى المجرم او مساعديه ، وغالبا ما يتم استهداف ضعاف افراد المجتمع وخاصة كبار السن ، لذلك يجب ان يسأل كبار السن والمعولين عما اذا كانوا قد التقوا بالمستفيد ام لا ، وتتضمن معظم عمليات الاحتيال اعتقاد الضحية بأنه سيحصل على نوع من المكاسب المالية أو انه يساعد احد الاصدقاء او الاقرباء .

يتضمن الملحق رقم (4)

ثاني عشر: التقارير

يجب أن يقدم مدير دائرة مكافحة غسل الاموال وتمويل الارهاب تقارير وبشكل دوري الى لجنة المجلس المختصة بحيث تغطي هذه التقارير المجالات التالية على الأقل:

1. الخروقات والتوصيات
2. التغييرات في موظفي / انظمة الدائرة .
3. الغرامات التي قد يتعرض لها البنك والسبب .
4. احصائيات عن أنشطة مكافحة غسل الاموال والاعمال التي تمت خلال العام .
5. منهجية الفحص على القوائم واي تغييرات جوهرية في تصنيف مخاطر العملاء .
6. تقييم مخاطر الاعمال (بما في ذلك المخاطر المتأصلة وسجلات المخاطر المتبقية) المنع والكشف والمعالجة وعلاقات العمل التي تم انهاؤها.
7. التدريب والتطوير في مجال مكافحة غسل الاموال وتمويل الارهاب والاحتيال .
8. التقارير الفورية عن اي مخاطر عالية متعلقة بغسل الاموال وتمويل الارهاب والعقوبات ذات الصلة.
9. تقييم مدى كفاية وفعالية سياسات واجراءات وانظمة البنك والضوابط الرقابية التي تمنع او تحول دون التورط في عمليات غسل اموال وتمويل ارهاب.
10. الاشارة في التقرير النصف سنوي عن حالات الابلاغ الداخلي والخارجي .
11. نتائج عملية التقييم الذاتي لمخاطر منتجات وخدمات البنك .
12. التطويرات والتحسينات في بيئة مكافحة غسل الاموال وتمويل الارهاب .

ثالث عشر: التدريب والتوعية

1. يجب أن يتوفر لدى البنك، برامج تدريبية مناسبة لمكافحة غسل الاموال وتمويل الارهاب بشكل مستمر.
2. يشمل البرنامج التدريبي كافة موظفي البنك بمختلف مستوياتهم

3. تعقد البرامج التدريبية بشكل متكرر بما يحفظ المستوى الكافي من المعرفة والأهلية للموظفين وفق مخطط ضابط الاتصال السنوي.
4. يتعين على كافة موظفي البنك حضور البرنامج التدريبي المقرر في مجال مكافحة غسل الاموال وتمويل الارهاب
5. يتم التدريب بالتنسيق مع دائرة التدريب، حسب البرنامج المعد من قبل ضابط اتصال مكافحة غسل الاموال وتمويل الارهاب لكافة موظفي البنك، وبما يشمل المدراء والمراقبين، موظفي العمليات، موظفي الصناديق، موظفي خدمة العملاء والتمويل ذوي العلاقة المباشرة مع الجمهور، الموظفين الجدد، موظفي خط الدفاع الثاني بما في ذلك موظفي مكافحة غسل الاموال وتمويل الارهاب وخط الدفاع الثالث.
6. يتم تصميم البرامج بما يتناسب مع احتياجات كل مستوى ووظيفة في البنك، ويشتمل على مجموعة من المحتويات كما هو مبين بالملحق رقم (5).
7. يتم مراجعة وتحديث المواد التدريبية الخاصة بمكافحة غسل الاموال وتمويل الارهاب سنوياً على الاقل وعند الحاجة وفي حال حدوث تغييرات في القانون أو التعليمات.

رابع عشر: حفظ السجلات والمستندات

وفقاً لأحكام المادة (10) من القرار بقانون لمكافحة غسل الاموال وتمويل الارهاب، يحتفظ البنك بجميع السجلات والمستندات لمدة لا تقل عن عشر سنوات من تاريخ الشروع أو انتهاء المعاملة المالية أو انتهاء علاقة العمل او حسب التعليمات الادراية بالخصوص على ان يكون الحد الادنى كما هو منصوص عليه بالقانون. وتكون قواعد التعامل مع السجلات والمستندات وفق الملحق رقم (6)

خامس عشر: ملكية السياسة :

تكون دائرة مكافحة غسل الاموال وتمويل الارهاب هي الجهة المالكة للسياسة واجراء التعديلات عليها وتحديثها عند الحاجة.

سادس عشر : المراجعة والتحديث :

1. يتم مراجعة هذه السياسة سنوياً من قبل دائرة مكافحة غسل الاموال وتمويل الارهاب، كما يتم مراجعتها عند حدوث تغييرات قانونية أو اصدار تعليمات جديدة أو لوائح أو توجيهات أو ممارسات دولية جوهرية تؤثر في هذه السياسة، وعند حدوث تغييرات داخلية في البنك تشمل على سبيل المثال لا الحصر إدخال / تغيير / إيقاف خدمات / عمليات جديدة أو عمليات إعادة تنظيم ...الخ تتطلب تحديثاً على هذه السياسة.
2. يجب توثيق جميع التعديلات أو الاضافات أو الحذف الذي يتم على السياسة بشكل رسمي وواضح، بحيث يتم الاحتفاظ بجميع نسخ السياسة، مع ضبط نسخها بما يبين رقم النسخة وتاريخها (اعداد/ تحديث)، تاريخ ورقم محضر الاجتماع الذي اعتمدت فيه السياسة، وجهة الاعتماد.
3. تعتمد السياسة وتعديلاتها أو تحديثاتها من مجلس الادارة وبتوصية من اللجنة المختصة التي تتبع لها دائرة مكافحة غسل الاموال.

انتهى

ملحق رقم "1" المرجعية القانونية

أولا: التشريعات والتعليمات الفلسطينية:

1. قرار بقانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39) للعام 2022 بتاريخ 2022/8/16.
2. مرسوم رئاسي رقم (14) لسنة 2022 بشأن تنفيذ قرارات مجلس الأمن.
3. تعليمات مكافحة غسل الأموال وتمويل الإرهاب الخاصة بالمصارف رقم (2016/3) الصادرة عن اللجنة الوطنية لمكافحة غسل الأموال وتمويل الإرهاب.
4. قرارات مجلس الوزراء بشأن الشركات غير الربحية.

ثانيا : التوصيات والتعليمات الإقليمية والدولية:

1. توصيات مجموعة العمل المالي الفاتف (FATF) بشأن مكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح، والمذكرات التفسيرية المتعلقة بها.
2. المعايير المالية للجنة بازل للسيطرة على ظاهرة غسل الأموال.
3. اتفاقية فيينا فيما يتعلق بالإتجار الغير المشروع بالمخدرات والمؤثرات العقلية.

ملحق رقم "2" **مراحل جريمة غسل الاموال وتمويل الارهاب**

يقصد بها الآليات أو العمليات التي يقوم بها غاسلوا الأموال لاخفاء المصدر غير الشرعي للاموال أو لتمويل الارهاب، والتي تمر عبر 3 مراحل، وتحتوي كل مرحلة على عدد من العمليات، على النحو التالي :

1. **مرحلة الإحلال Replacement :**

وتهدف الى ادخال الاموال غير المشروعة الى النظام المصرفي عبر عدة طرق ابرزها شراء العقارات ، التهريب عبر الحدود ، فتح حسابات وهمية .

2. **مرحلة التغطية والتموي Layering :**

تتم من خلال عدة مراحل وعمليات معقدةضمن عدة عمليات بنكية لتظهر أنها أموال ناتجة عن أعمال مشروعة مثل تحويل الاموال إلى حسابات في بنوك أخرى على أنها دفعات لعمليات شراء بضاعة.

3. **مرحلة الدمج: Integration**

يتم في هذه المرحلة إعادة ضخ الأموال إلى الاقتصاد من خلال أعمال مشروعة وقانونية وخلطها مع أموال مشروعة وعندها تظهر بشكل أموال متأتية من أعمال مشروعة وتكون صعبة التمييز والفصل. مثل القيام بإصدار اعتماد لاستيراد بضائع، أخذ قرض لبناء إسكان أو شراء سيارة... الخ.

4. يعد مرتكبا لجريمة غسل الاموال كل من قام باستبدال او تحويل او نقل الاموال من قبل اي شخص وهو يعلم بأن هذه الاموال تشكل متحصلات لجريمة لغرض اخفاء او تمويه الاصل غير المشروع لهذه الاموال ، او مساعدة اي شخص متورط في ارتكاب الجريمة الاصلية للتهرب والافلات من التبعات القانونية المترتبة على افعاله ، وكذلك تملك الاموال وحيازتها من قبل اي شخص وهو يعلم في وقت الاستلام ان هذه الاموال هي متحصلات جرمية .
5. يعد مرتكبا لجريمة تمويل الارهاب كل شخص يقوم عمدا بتقديم او جمع الاموال من مصدر مشروع او غير مشروع بأي وسيلة كانت مباشرة او غير مباشرة وبنية غير مشروعة لاستخدامها أو مع علمه بأنه سيتم استخدامها جزئيا او كليا في ارتكاب اعمال ارهابية من قبل شخص ارهابي او منظمة ارهابية .

ملحق رقم "3" مؤشرات / أساليب عملية غسل الاموال وتمويل الارهاب

(مؤشرات الخطر)

1. **فتح الحسابات:**

1.1. عملاء يطلبون فتح حساب في الفرع البعيد عن مكان عملهم أو سكنهم دون مبرر، بالرغم من وجود فرع آخر أقرب للعميل.

1.2. العملاء الذين يفتحون حسابا للاستعمال المؤقت.

1.3. عملاء يفتحون حساباً باسم غير اسم المستفيد الحقيقي من الحساب.

1.4. العملاء الذين يظهرون قوائم مالية لا تتناسب مع القوائم المالية المتعارف عليها لمثل نشاط العميل.

1.5. العملاء الذين يتقدمون للبنك كممثلي لشركات تعمل في مناطق تشتهر بوجود الأنشطة غير القانونية أو مصنفة بأنها دول غير متعاونة في مجال مكافحة غسل الأموال وتمويل الإرهاب.

1.6. العملاء الذين يطلبون استثنائهم من متطلبات التعرف على هوية العميل.

1.7. امتناع العميل عن تزويد البنك باثبات شخصية واضحة او معلومات اخرى تتطلبها اجراءات اعرف عميلك أو تقديم معلومات غير صحيحة.

1.8. يتوجب اتخاذ ما يلزم للتعرف على المستفيد الحقيقي من الحساب في حال :

- عند الشك بقيام العميل بالتصرف نيابة عن شخص اخر
- عدم قدرة البنك على الحصول على مستندات او معلومات عن المستفيد الفعلي من الحساب.
- اختلاف طبيعة حركة الحساب عن طبيعة نشاط العميل.
- طلب العميل تنفيذ عمليات مالية لمنفعة مستفيد اخر لا تربطه به علاقة واضحة دون مبررات او اسباب مقنعة .

2. **عمليات السحب والإيداع:**

2.1. إيداعات نقدية كبيرة تبدو غير منطقية وغير منسجمة مع نشاط العميل وحركة حسابه.

2.2. تركيز العميل على السحوبات والإيداعات النقدية عوضا عن وسائل السحب والدفع الأخرى.

2.3. تبديل كميات كبيرة من الأوراق النقدية ذات الفئة الصغيرة لفئات كبيرة دون مبرر.

2.4. إيداع العميل لأوراق نقدية تحمل أرقام متسلسلة والتي تدل أن الأموال بقيت كما هي من مصدرها دون أن تُستخدم من قبل الآخرين.

2.5. تنفيذ سحوبات كبيرة على الحساب بالمقارنة مع حركة السحوبات الاعتيادية للعميل دون مبرر.

2.6. إيداع مبالغ نقدية كبيرة من خلال الصراف الآلي لتجنب الاتصال المباشر بالموظف، خصوصا إذا كانت هذه الإيداعات غير منسجمة مع حركة الحساب.

2.7. إيداع مبالغ كبيرة ومن عدة أشخاص مختلفين على نفس الحساب وقد تكون إيداعات صغيرة ولكن مجموعها كبير دون مبرر مقبول لهذه الإيداعات لذا لا يُسمح بإيداع أية مبالغ نقدية في حساب العميل إلا من قبل العميل نفسه أو من يفوضه العميل بذلك رسميا.

3. **العمليات المصرفية التي تتعلق بالمفوضين عن الحساب:**

3.1. احتفاظ العميل بأكثر من حساب.

3.2. توزيع الإيداعات النقدية على أكثر من حساب بحيث تشكل بمجموعها مبالغ كبيرة لا تتناسب مع طبيعة عمل العميل أو نشاطه.

3.3. فتح عدة حسابات لدى عدد من المصارف تعمل بنفس المنطقة الجغرافية ومن ثم تجميعها في حساب واحد من خلال تحويل الأرصدة إلى حساب واحد ومن ثم تحويلها إلى الخارج.

3.4. ايداعات ثابتة في الحساب ثم تحويل المال المتجمع.

3.5. تأسيس العميل لمؤسسات تجارية أو مالية أو اجتماعية أو غير ربحية لا تتناسب مع أهدافه ونشاطه.

3.6. التغيُرات غير المبررة في نشاط العميل.

3.7. التردد في إعطاء المعلومات عن الأنشطة وأطراف العلاقة بالنشاط.

3.8. اكتشاف وثائق غامضة أو غير قانونية خلال التعامل مع العميل.

3.9. قيام العميل بفتح حسابات باسم مؤسسات غير مقيمة وتفويضه بإدارة هذه الحسابات.

3.10. اختلاف بيانات العميل المالية التي يقدمها عن نشاطه عن البيانات المعروفة لمثل هذا النشاط.

4. **حركة الحساب:**

4.1. حدوث نشاط كثيف على الحساب

4.2. تغير مفاجيء في حركة الحساب بحيث يتعارض مع النشاط التاريخي للحساب.

4.3. تحويلات متعددة من وإلى الحساب نفسه.

4.4. عدم تحسس العميل أو اهتمامه للتكاليف التي تترتب على الحساب نتيجة الحركة عليه.

4.5. إيداعات من قبل عدة أشخاص على نفس الحساب دون أن يكون لهم علاقة عمل مبررة.

4.6. أسماء كفلاء أو معرفين يصعُب الوصول لهم.

4.7. مخاطبة البنك من خلال الفاكس أو كتب خطية لتفادي الاتصال المباشر مع العميل

5. **العمليات المصرفية التي تتعلق بالشيكات والحوالات الالكترونية:**

5.1. إيداع شيكات (أطراف ثالثة) تكون مجيرة لصالح صاحب الحساب دون وجود انسجام فيما بين الأطراف في طبيعة العمل.

5.2. تكرار إيداع شيكات أجنبية أو سياحية بالحساب لا تتناسب مع نشاط العميل وحركة حسابه وبشكل غير اعتيادي.

5.3. إيداع شيكات بمبالغ ضخمة مجيرة باسم صاحب الحساب.

5.4. إيداعات كبيرة بالحساب بأي من الوسائل تبدو غير منطقية وغير منسجمة مع نشاط العميل وحركة الحساب.

5.5. تحويلات متكررة وغير مبررة لحسابات في بنوك أخرى سواء محلية أو خارجية.

5.6. تحويلات متكررة أو منتظمة بمبالغ متماثلة أو بأرقام صحيحة .

5.7. تحويلات بمبالغ صغيرة عبر الادوات والوسائل الالكترونية لعدة أشخاص دون مبرر.

5.8. تجميع تحويلات الكترونية بالحساب ثم اعادة تحويلها لشخص أو أشخاص آخرين أو لبلد آخر.

5.9. تحويلات إلى بنوك متواجدة في بلاد ذات قوانين صارمة للحفاظ على السرية المصرفية.

5.10. التحويلات إلى الخارج والمصحوبة بتعليمات بالدفع النقدي.

5.11. الحوالات الواردة لحساب عميل بمبالغ ضخمة ولا تتناسب مع طبيعة نشاط العميل.

5.12. الحوالات الصادرة والواردة إلى دول لا تلتزم بتطبيق قوانين مكافحة غسل الأموال وتمويل الارهاب، أو تشتهر بتجارة المخدرات وغيرها من الأعمال الإجرامية.

5.13. الحوالات الواردة على الحساب لمنفعة طرف ثالث.

5.14. تنفيذ حوالة غير روتينية ضمن حزمة حوالات روتينية.

6. <u>الحوالات الفورية:</u>

6.1. اظهار القلق الشديد من قبل المرسل لمتطلبات الافصاح عن الحركة

6.2. تردد المرسل أو رفضه تقديم المعلومات أو معلومات اضافية أو تقديم معلومات خاطئة أو منقوصة

6.3. الغاء المرسل للحوالة بعد طلبها بسبب متطلبات الافصاح عن المعلومات المطلوبة

6.4. عدم وجود علاقة مبررة بين المرسل والمستفيد

7. <u>العمليات المصرفية التي تتعلق بالتسهيلات الائتمانية:</u>

7.1. التردد في إعطاء المعلومات عن الأنشطة وإطراف العلاقة بالنشاط.

7.2. اكتشاف وثائق غامضة أو غير قانونية خلال التعامل مع العميل.

7.3. قيام العميل بفتح حسابات باسم مؤسسات غير مقيمة وتفويضه بإدارة هذه الحسابات.

7.4. طلب قروض بمبالغ ضخمة مقابل رهن أصول أو ممتلكات أو ودائع موجودة بالخارج مسجلة باسم العميل أو مسجلة باسم أطراف خصوصا إذا تواجدت هذه الأصول ببلد تشتهر بظاهرة غسل الأموال وتمويل الارهاب.

7.5. السداد المبكر أو المفاجئ للقروض وخاصة المشكوك في تحصيلها أوتسديد دفعة كبيرة من القرض بشكل مفاجئ

7.6. التقدم بطلب الحصول على تسهيلات لشركات تعمل في مناطق offshore أو مضمونة بالتزامات بنوك أو مؤسسات تعمل في هذه المناطق.

7.7. القروض الممنوحة لمنفعة طرف ثالث أو بيعها لطرف ثالث دون مبرر.

7.8. تقديم ضمانات إضافية كرهن أصول أو تقديم كفالات من قبل أشخاص لا ترتبط نشاطاتهم معا.

7.9. عدم الاهتمام بتسديد أقساط قرض/ قروض ممنوحة بضمان تأمينات نقدية.

7.10. الحصول على قرض لمنفعة طرف ثالث غير مبرر أو تحويل القرض لطرف ثالث.

8. <u>عمليات الإعتمادات المستندية وخطابات الضمان ومستندات التحصيل:</u>

8.1. فتح إعتمادات مستندية بمبالغ لا تتناسب مع ثمن البضائع التي سيستوردها العميل.

8.2. تسييل خطابات الضمان بعد فترات قصيرة.

8.3. فتح إعتمادات مستندية بمبالغ كبيرة لا تتناسب مع طبيعة نشاط العميل وحجمه، أو أن يكون المستفيد منها من اقرباء العميل.

8.4. طلب العميل تعديل مكان دفع قيمة الاعتماد المستندي وذلك لصالح أطراف أخرى مقيمة خارج بلد المستفيد.

8.5. طلب العميل تعديل اسم المستفيد من الاعتماد قبل الدفع مباشرة.

9. <u>تأسيس شركات لا تتناسب مع أهداف ونشاط العميل</u>

أن يكون نشاط العميل في مناطق جغرافية معروفة بكثرة الجرائم التي ينتج عنها أموال غير مشروعة أو مناطق صراعات وخلافات سياسية حيث يزيد الابتزاز والجرائم والمناطق التي تنتشر فيها العصابات والاتجار بالمخدرات والتهريب وعمليات التزوير وغيرها من الأنشطة الإجرامية التي ينتج عنها أموال ضخمة لابد أن يتم تبييضها.

10. صناديق الامانات:

يتوجب على الموظف المختص بصناديق الأمانات أن يكون على علم بشكل عام بالمقتنيات والمواد التي يرغب العميل بحفظها في الصندوق بطريقة لبقة ودون لفت نظر العميل ، وفي حال الإشتباه سؤال العميل عن طبيعة المواد المراد حفظها ، وفي حال توافر مؤشرات مقبولة وحسب التالي ، إبلاغ دائرة مكافحة غسل الاموال حسب الأصول.

11. إستغلال الصندوق في عملية ايداع نقد و او شيكات بغرض التهرب من ايداعها بالحساب .

11.1. إحتفاظ العميل بعدة صناديق أمانات دون مبرر واضح.

11.2. إستخدام صناديق الأمانات بشكل كبير مما يشير الى إحتفاظ العميل بكميات كبيرة من النقد في هذه الصناديق.

11.3. قيام العميل بشكل متكرر بزيارة الصندوق قبل أو بعد قيامه بإيداعات نقدية تقل عن الحد الأدنى المحدد في التعليمات.

12. المعاملات ذات الصلة بالاستثمار:

12.1. استخدام الحساب الاستثماري لغايات تحويل الاموال لجهات خارجية وخاصة مناطق offshore

12.2. التعامل بالاوراق المالية بما لا يتناسب مع نشاط ووضع العميل.

12.3. ادخال أموال من الخارج ثم شراء اوراق مالية.

12.4. شراء الاوراق المالية بمبالغ واردة من الخارج ثم بيعها.

ملحق رقم "4" سياسة واجراءات مكافحة ومنع الاحتيال

أولا :المقدمة :

مخاطر الاحتيال والاختلاس والتزوير تشمل كافة قطاعات الاعمال ولا تقتصر على أي مؤسسة بعينها في القطاع الخاص سواءً كانت المؤسسة مالية أو صناعية أو خدماتية، اضافة الى ذلك أن التلاعب / الاحتيال / الاختلاس / التزوير يتكيف مع المتغيرات التي قد تطرأ على أي قطاع، فبالرغم من آليات التدقيق الداخلي والمراقبة والتقصي وشروط مراجعي الحسابات الخارجيين المستقلين وقواعد السلوك المهني ، يستمر حدوث التلاعب والاحتيال والاختلاس والتزوير ، ويحدث الاحتيال على العملاء عندما يقنع المجرمون العملاء او يخدعونهم لتحويل اموال الى المجرم او مساعديه ، وغالبا ما يتم استهداف ضعاف افراد المجتمع وخاصة كبار السن ، لذلك يجب ان يسأل كبار السن والمعولين عما اذا كانوا قد التقوا بالمستفيد ام لا ، وتتضمن معظم عمليات الاحتيال اعتقاد الضحية بأنه سيحصل على نوع من المكاسب المالية أو انه يساعد احد الاصدقاء او الاقرباء .

ثانيا: الاهــداف :

أعدّت هذه السياسة لتحقيق الاهداف التالية :

1. الحدّ من التلاعب/ الاحتيال/الاختلاس/التزوير داخل البنك .
2. انشاء اجراءات عمل واجراءات رقابية للتعامل مع حالات التلاعب / الاحتيال / الاختلاس / التزوير حال وقوعها.
3. الحد من المخاطر والتأثير الممكن حصوله نتيجة عمليات التلاعب / الاحتيال / الاختلاس / التزوير.
4. إسترداد الخسائر الناشئة عن عمليات التلاعب / الاحتيال / الاختلاس / التزوير.
5. خلق (انشاء) ثقافة وبيئة تشجع على تخفيض التلاعب / الاحتيال / الاختلاس / التزوير.
6. تحديد المسؤوليات في الابلاغ وإتخاذ الخطوات المناسبة للأحداث الناشئة عن حالات الاحتيال والتزوير والتلاعب والاختلاس.

ثالثا: أنواع الاختلاس

1. **عمليات الإختلاس الداخلي:**

ويقصد به الإختلاس الذي يتم من قبل موظف او موظفين البنك من حسابات البنك و/او العملاء سواء كانوا بمفردهم أو بالتعاون مع أفراد خارج البنك.

2. **عمليات الإختلاس الخارجية:**

على الرغم من كونها أقل شيوعا من تلك التي تتم داخليا إلا أننا نجد ظهورها بخطى سريعة نتيجة اتساع استخدام بعض أنواع التكنولوجيا المتقدمة مثل اتساع نطاق ومجال تهريب بطاقات الإئتمان المسروقة وإمكانية الحصول على بطاقات سليمة على الرغم من وجود مخالفات في عملية إصدارها.

رابعا: طرق الاختلاس

1. الاختلاس المباشر
2. الاختلاس المقترن بحيلة
3. القيام باعمال غير اصوليه بقصد التكسب غير القانوني مثل :-
   3.1. شراء مواد مخالفة للمواصفات
   3.2. اجراء صيانات وهمية للسيارات
   3.3. صرف قيمة اعمال وهمية
   3.4. التزوير تمهيدا للاختلاس.
   3.5. استبدال المواد بمواد اقل جودة.
   3.6. اتلاف الحسابات او الاوراق.
   3.7. التلاعب بالحسابات: السحب من أحد الحسابات واستغلال الاموال ومن ثم ايداع المبلغ لاحقا في حساب آخر ومن ثم سحب شيك على الحساب الثاني وايداعه في الحساب الاول كتغطية لعملية السحب الاولى وتنجح هذه العملية لكون المختلس يحمل صلاحية ادارة الحسابين المعنيين.
   3.8. التلاعب بالايداعات: قيام الموظف باختلاس مبلغ من عميل عند ايداع هذا المبلغ من ثم يتم تغطية جزء من المبلغ المختلس من ايداع شخص آخر ومن ثم شخص ثالث وهكذا, حيث أن الموظف المختلس يقوم بتسجيل تفاصيل تلك العمليات المختلسة في سجل يحتفظ به.

خامسا: الانواع الشائعة للاحتيال على العملاء

1. خدعة الرسوم المدفوعة مسبقا : يطلب من الضحية دفع الرسوم مقدما مقابل الخدمات المالية التي لا تقدم على الاطلاق .
2. خدعة مكافحة الفيروسات : يتصل المحتال بصفته من شركة برمجيات معروفة بالضحية مدعيا انه تم اكتشاف فيروس على جهازه ، ولازالة هذا الفيروس يطلب تحويل مبلغ مالي عبر حوالة بنكية او بطاقة ائتمان .
3. خدعة المؤسسات الخيرية : يتم التواصل مع الضحية من خلال شخص يطلب ارسال تبرع الى احد الافراد لمساعدة ضحايا احد الاحداث (حرب / كوارث طبيعية ...) .
4. خدعة الحالات الطارئة : يتم استدراج الضحية للاعتقاد بانهم يرسلون الاموال لمساعدة احد الاقارب او الاصدقاء الذي يعاني من ظرف طارئ .
5. خدعة التوظيف : تستجيب الضحية لاعلان عن وظيفة وهمية ، ويقوم المحتال بارسال شيك بقيمة تفوق قيمة نفقات التوظيف ، ويطلب من الضحية اعادة ارسال المتبقي من الشيك عبر حوالة مالية ، وعند اعادة الشيك تصبح الضحية مسؤولة عن كامل قيمة الشيك .
6. خدعة الشيكات المزورة : غالبا ما يتم ارسال شيك للضحية كجزء من خدعة ، ويطلب منه ايداع الشيك واستخدام قيمته لدفع نفقات وظيفة او الشراء عبر الانترنت ، وتبقى الضحية مسؤولة عن كامل قيمة الشيك بعد اعادته .

7. خدعة الاجداد : يتم التواصل مع الضحية من قبل المحتال مدعيا انه حفيد يعاني من ضائقة / خبير طبي / ضابط تطبيق قانون / محام ، ويتم الوصف للضحية بأن هناك حالة طارئة / كفالة / نفقات سفر ويطلب ارسال حوالة مالية سريعة .
8. خدعة الهجرة : يتم التواصل مع الضحية من قبل المحتال بصفته موظف في دائرة الهجرة باعاء وجود مشكلة في سجل الهجرة الخاص بالضحية ، ويطلب منه تسديد دفعة فورية لتسوية المشكلة مع التهديد بالسجن / الترحيل في حال عدم التحويل بسرعة .
9. خدعة الشراء عبر الانترنت : ترسل الضحية الاموال لشراء سلعة عبر الانترنت عبر مواقع وهمية ، وبعد ارسال الحوالة ، لا تستلم الضحية البضاعة المطلوبة .
10. خدعة الضرائب : يتم التواصل مع الضحية من قبل المحتال بصفته موظف مصلحة ضرائب / وكالة حكومية بادعاء انه مدين لمصلحة الضرائب ويتوجب دفعها فورا لتلافي السجن / الترحيل / تعليق رخصة القيادة .
11. خدعة اليانصيب / الجوائز : يتم ابلاغ الضحية بأنها فازت بجائزة يانصيب او سباق خيل ، ويطلب منها ارسال حوالة مالية لتغطية الرسوم والضرائب على الجائزة.
12. خدعة العلاقات : يتم استدراج الضحية للاعتقاد بانها على علاقة شخصية مع شخص التقته عبر الانترنت او مواقع التواصل الاجتماعي او مواقع المواعدة ، وغالبا ما يتم استغلال الضحية عاطفيا للاعتقاد بانها ترسل الاموال لخطيبها لتغطية مصاريف السفر او نفقات طبية .
13. خدعة عقار للايجار : ترسل الضحية الاموال من اجل ايجار عقار وهمي او قد يكون مالك العقار هو نفسه ضحية عبر قيام المحتال بارسال شيك تفوق قيمته قيمة الايجار ويطلب من الضحية اعادة الفرق .
14. مواقع التواصل الاجتماعي : وتشمل حالات الاحتيال التي تتم من خلال التعارف الوهمي عبر مواقع التواصل الاجتماعي.
15. العملات الافتراضية او الرقمية : وتشمل الاتجار غير المشروع بالعملات الافتراضية بذريعة الربح السريع والعالي النسبة .

سادسا: المبادئ الرئيسية

1. **اعتمد البنك الاسلامي العربي الاتي للحد من مخاطر الاحتيال / الاختلاس / التزوير :**
   1.1. انظمة ملائمة وفعّالة للرقابة المالية والادارية.
   1.2. انشاء دائرة للتدقيق الداخلي بصلاحيات واضحة ومحددة للتأكد من أن النظام المالي يعمل بفاعلية.
   1.3. تعيين مدققين داخليين مستقلين لتقديم المشورة واستعراض التقارير الخاصة وتطوير الاجراءات الواجب اتباعها من قبل طاقم مختص في حالات الاشتباه بعمليات التلاعب / الاحتيال / الاختلاس / التزوير.
   1.4. انشاء خطة عمل تظهر الاجراءات الواجب اتباعها لحالات الاشتباه و/ او اكتشاف حالات تلاعب/ احتيال / اختلاس / تزوير.
   1.5. نشر الوعي المناسب في ما يخص عمليات التلاعب / الاحتيال / الاختلاس / التزوير بحيث يجب على جميع الموظفين الامتثال والعمل بها.
   1.6. اجراء مراجعة دورية للاجراءات الرقابية واجراءات العمل لتقييم اليات الحد من خطر التلاعب/الاحتيال/الاختلاس/التزوير بحيث تشمل جميع وظائف وعمليات البنك وتعالج هذه المراجعة المخاطر

الناجمة عن عمليات التلاعب/ الاحتيال/ الاختلاس/التزوير الداخلي والخارجي على حد سواء وان تحدد مستوى وطبيعة تعرض البنك لمخاطر التلاعب/ الاحتيال/ الاختلاس/ التزوير.

1.7. ان تخضع جميع المنتجات والخدمات الجديدة لعملية التقييم, إضافة الى مراجعة وتقييم المخاطر لكافة أدلة السياسات والاجراءات المتعلقة بتلك المنتجات والخدمات لمعرفة إذا ما قد تم تخفيف مخاطر عمليات التلاعب / الاحتيال / الاختلاس / التزوير وذلك لتكون قادرة على تحديد وتقييم مخاطر عمليات التلاعب / الاحتيال / الاختلاس / التزوير وبيان ما هي التدابير التي اتخذت والاجراءات التي ما زالت هناك حاجة لاتخاذها لتقليص وتخفيف هذه المخاطر.

2. <u>نظام الرقابة الداخلية:</u>

اجراءات الرقابة الداخلية (مثل الاجراءات الرقابية الناتجة عن إدارة المخاطر, التدقيق الداخلي الشامل, ضوابط الميزانية, الفصل بين المهام, الضوابط والتعليمات الداخلية والاشراف على الموظفين) قد صممت للتقليل والتخفيف أو منع حدوث عمليات التلاعب / الاحتيال / الاختلاس / التزوير وآثارها المتوقعه , وتتضمن الكشف الفوري لحالات التلاعب / الاحتيال / الاختلاس / التزوير.

ويمكن كشف وتخفيض أو منع عمليات التلاعب / الاحتيال / الاختلاس / التزوير اذا كانت الاجراءات الرقابية قوية وتطبق باستمرار وبشكل فعّال وناجح وشفاف, مع ضرورة وجود الضوابط والرقابة الروتينية من قبل الادارة .

3. <u>الطاقم / التدريب</u>

إن تعيين طاقم موظفين مناسب في البنك الاسلامي العربي, وتبني افضل الاجراءات الرقابية واجراءات العمل والتقيد التام بها هو خط الدفاع الاول في حماية المؤسسة من عمليات التلاعب / الاحتيال / الاختلاس / التزوير, كما أن وعي الموظفيين ومعرفتهم في سياسة التلاعب / الاحتيال / الاختلاس / التزوير والاجراءات المعمول بها هي الوسيلة الاساسية لانظمة تشغيل فعّالة.

4. <u>الابلاغ والتحقق</u>

إن وجود اجراءات مناسبة ومستمرة للابلاغ والتحقق تعتبر في غاية الأهمية في عملية اكتشاف حالات التلاعب / الاحتيال / الاختلاس / التزوير, حيث قام البنك الاسلامي العربي بانشاء خطة عمل للابلاغ والتحقق في كل حالات التلاعب / الاحتيال / الاختلاس / التزوير المشكوك فيها وتتمثل على سبيل المثال في إبلاغ الجهات الرقابية.

من المهم أن تعالج عمليات التحقق في سرية تامة, ولكن على الادارة ضرورة الافصاح عنها للموظفين في الوقت المناسب لتعلم الدروس والعبر من كل حالات التلاعب / الاحتيال / الاختلاس / التزوير يتم التعرض لها.

<u>سابعا: المسؤوليات</u>

1. <u>مسؤولية الاعداد:</u>

دائرة مكافحة الاحتيال وغسل الاموال وتمويل الارهاب هي المسؤولة عن إعداد سياسة منع الاحتيال و التزوير وآليات العمل بها ورفعها للسيد المدير العام للتوصية بإعتمادها من لجنة المجلس المختصة .

2. **مسؤولية التدريب :**

دائرة الموارد البشرية والتدريب هي المسؤولة عن التنسيق مع دائرة مكافحة الاحتيال وغسل الاموال وتمويل الارهاب لاعداد الورش والدورات الخاصة لتريب موظفي البنك الاسلامي العربي على آليات اكتشاف حالات التلاعب / الاحتيال / التزوير / الاختلاس .

3. **مسؤولية التحديث:**

دائرة مكافحة الاحتيال وغسل الاموال وتمويل الارهاب هي المسؤولة عن تحديث سياسة منع الاحتيال والتزوير والتلاعب والاختلاس وآليات العمل بها .

4. **مسؤولية الابلاغ للجهات الرسمية:**

تقوم دائرة مكافحة الاحتيال وغسل الاموال وتمويل الارهاب بابلاغ وحدة المتابعة المالية عن حالات الاحتيال ، فيما تقوم دائرة ادارة المخاطر بابلاغ سلطة النقد والجهات الاخرى ذات العلاقة.

ثامنا: أنظمة الابلاغ المتبعة للحالات المشتبه بها

عند اكتشاف حالة احتيال و/أو تزوير و/أو اختلاس و/أو تلاعب قام بها موظف في أي وحدة عاملة من وحدات البنك يتم إجراء التالي:

1. يتم اعلام السيد المدير العام أو من ينوب عنه حال غيابه هاتفيا بالواقعة.
2. يتم إرسال مذكرة سرية من مسؤول الوحدة الأول إلى السيد المدير العام بواسطة البريد اليدوي ونسخة منها لمدير إدارة المخاطر ومدير دائرة التدقيق الداخلي.
3. إن كان مكتشف الحالة موظف في فرع و/أو دائرة والفاعل هو المسؤول الأول للفرع و/أو الدائرة يقوم الموظف مكتشف الحالة مباشرةً بإبلاغ كلّ من مدير إدارة المخاطر ومدير التدقيق الداخلي الذين بدورهما يقومان سويا ومباشرة بإعلام المدير العام ومن ثم تقييم الحالة وتحويلها للسيد المدير العام بسرية تامة وإجراء الخطوات المذكورة أدناه.
4. يقوم السيد المدير العام بتحويل الحالة إلى لجنة تقصي الحقائق في البنك وتفويضها باجراء ما يلزم لانجاز مهمتها على أكمل وجه مع ضرورة اشعار دائرة مكافحة الاحتيال وغسل الاموال وتمويل الارهاب .
5. يقوم المدير العام بتبليغ رئيس مجلس الإدارة و سلطة النقد الفلسطينية فورا بالحالة المكتشفة بالتنسيق مع الإدارة العليا.
6. يقوم المدير العام بتبليغ شركة التأمين عن الحادثة "إن كانت مغطاة بالغطاء التأميني" وذلك حفاظا لحقوق البنك في المطالبة التأمينية بالتنسيق مع الادارة العليا، وذلك خلال شهر كحد أقصى من تاريخ التحقق الفعلي للحادثة.
7. يقوم المدير العام بتبليغ الجهات الأمنية المختصة "تبعا للحالة المكتشفة" بالتنسيق مع الادارة العليا.
8. تقوم لجنة تقصي الحقائق باجراء ما يلزم من تحديد المسؤوليات، وتحديد الأشخاص المراد تقصي الحقائق معهم.
9. تقوم اللجنة باجراء التحليل اللازم للحالة مرفقا بها الوثائق والمستندات المدعمة للحالة.
10. تقوم اللجنة برفع مقترحاتها وتوصياتها اللازمة وتبليغ دائرة إدارة المخاطر بحدث تشغيلي حسب الأصول.
11. تقوم دائرة إدارة المخاطر بعد تبليغها رسميا بالحالة بتبليغ سلطة النقد الفلسطينية رسميا بعد التنسيق مع المدير العام بتقرير تفصيلي يبين نتائج الحالة المكتشفة مضافا اليها النتائج والتوصيات والاجراءات المتخذة.
12. تقوم اللجنة بتحويل التقريرالنهائي للمدير العام.

13. يقوم المدير العام بتحويل التوصيات والاجراءات المتخذة للدوائر ذات الإختصاص لاجراء ما يلزم كلّ حسب اختصاصه، سواء في متابعة متطلبات شركة التأمين و/أو المباحث / النيابة العامة...إلخ.
14. يقوم السيد المدير العام بارسال تقرير لمجلس الإدارة بالتبليغ عن الحالة والمقترحات والتوصيات والإجراءات المتخذة لعلاج هذه الحالة والثغرات الناتجة عنها إن وجدت.

تاسعا : نشر الوعي المصرفي

يقسم الوعي المصرفي بعمليات التلاعب والإحتيال والتزوير إلى شقين(موظفي المصرف / عملاء المصرف)

1. الوعي المصرفي لموظفي المصرف:

1.1. قيام كل من دائرتي التدريب وغسل الاموال باجراء ورشات عمل توعوية لجميع موظفي الفروع والدوائر وعلى النحو التالي:
1.2. تعميم سياسة منع / تخفيض التلاعب/التزوير/الاختلاس من قبل دائرة التنظيم وإجراءات العمل على جميع موظفي البنك، والحصول على تأكيد خطي باطلاعهم عليها.
1.3. تقدم دائرة إدارة المخاطر شرحاً شاملاً لجميع الاجراءات الرقابية الرئيسية وكيفية سيطرتها على المخاطر ذات العلاقة.
1.4. تقدم دائرة إدارة المخاطر شرحاً لحالات الاحتيال والتزوير والتلاعب التي حدثت والاجراءات الرقابية ذات العلاقة سواء القائمة إن وجدت والتي تم استحداثها لتخفيض حدوث مثل هذه الحالات مستقبلا وذلك للإستفادة وأخذ العبر.
1.5. تقدم دائرة التدقيق الداخلي شرحاً شاملاً للأخطاء التي قد تتكرر والملاحظات الرئيسية التي تخفض البيئة الرقابية للفرع/الوحدة.

2. لعملاء المصرف:

2.1. عن طريق نشر نشرات تثقيفية أو دليل عن الآليات الواجب اتباعها عند تنفيذ أية عملية مصرفية وخصوصا العمليات الإلكترونية مثل استخدام الانترنت البنكي، بطاقة الصراف الآلي...إلخ، عبر أحد الوسائل التالية:
   - عن طريق شاشات الفروع الإلكترونية.
   - عن طريق موقع البنك الإلكتروني.
   - باستخدام منشورات ورقية يتم توفيرها في الفروع.
   - نشر سياسات وإجراءات مجلس الإدارة في تطبيق سياسات الحد من المخاطر في التقرير السنوي الصادر عن البنك.

عاشرا: ضوابط وقواعد لتخفيض وردع الاحتيال والتزوير والتلاعب

1. وضع ضوابط ومحددات واضحة وصريحة لإستخدامات الخدمات المصرفية الالكترونية.
2. وضع اجراءات رقابية قوية وفعّالة وعصرية لتكون خط الدفاع الرئيسي ضد أي عمليات تلاعب / احتيال / اختلاس / تزوير.

3. اعتماد مبدأ الرقابة الثنائية في تنفيذ أي عملية مصرفية.
4. عدم الافراط في الثقة بالآخرين والتحوط في التعاملات التجارية.
5. تشكيل لجنة مختصة محترفة لكشف حالات التزييف والاحتيال والتلاعب.
6. اصدار اجراءات لفتح الحسابات تعتمد على معيار الرقابة الثنائية.
7. اصدار قواعد للخدمات المصرفية الالكترونية.
8. اصدار دليل لمكافحة عمليات غسيل الاموال والاحتيال .
9. دراسة الشكاوي التقنية المتعلقة بالخدمات البنكية عن طريق الانترنت.
10. تحديث بيانات العملاء بشكل دوري.
11. نشر الوعي التام بعمليات الاحتيال والتزوير والتلاعب من خلال عقد الدورات التدريبية لموظفي البنك وعلى مختلف المستويات.
12. تطبيق قواعد التعامل مع الحسابات المصرفية (أعرف عميلك) KYC .
13. التأكيد على تطبيق خدمة الرسائل القصيرة (SMS) على كافة عملاء البنك.
14. التأكد من سلامة الشيكات المصرفية المستلمة بأستخدام الوسائل التنقية الحديثة.
15. المحافظة على وثائق الهوية وأية مستندات ومعلومات شخصية للعملاء وعدم تزويد أي جهة بنسخ منها إلا بموافقة العميل الخطية او قرار محكمة .
16. التأكد من صحة ودقة عناوين المواقع الالكترونية للبنوك والجهات المصرفية والمالية قبيل إجراء أية عملية مصرفية من خلالها.
17. تحصين أجهزة الحاسب الآلي والأنظمة البنكية ببرامج الحماية من الفيروسات والقرصنة والتأكد من تطوير تلك البرامج وتحديثها أولا بأول.
18. تغيير الأرقام السرية لأية أنظمة أو برامج معتمدة لدى البنك و بشكل دوري.
19. التحقق من شخصية العميل ، وذلك عند اجراء أية حركة مالية على حسابات العملاء مثل (السحب النقدي والتحويل الداخلي والخارجي...الخ) .
20. تدقيق توقيع العميل أو الشخص المفوض أو الوكيل تدقيقا أصوليا.
21. اعتماد آليات وإجراءات شحن النقد من وإلى الفرع بحيث تحدد من خلالها مواعيد الشحن والاشخاص المفوضين في ذلك وبسرية تامة مع تطبيق أعلى معايير الحماية والسلامة.
22. اصدار تعليمات ونماذج لقبول تنفيذ تعليمات على حسابات العملاء بموجب الفاكس وأية وسيلة اتصال مقبولة أخرى.
23. تدقيق التواقيع على كتب التزام تحويل الرواتب والتأكد من أن الشخص الموّقع هو المفوض.
24. تحديد صلاحيات التنفيذ على النظام بحيث يكون هنالك سقوف لكل موظف وبحسب المستوى الاداري.
25. رقابة ومراجعه ثنائية على الأعمال اليومية من خلال الحافظة اليومية التي يتم انشاؤها.
26. التأكد من صحة السويفت ومن التشفير الصحيح للرسالة واسم البنك والجهة المستفيدة لاغراض الحوالات والاعتمادات وبوالص التحصيل ... الخ.
27. تمرير مستندات الاعتمادات وبوالص التحصيل للفرع ليقوم بدوره بإبلاغ العميل، وتوقيعه بما يفيد استلامه للمستندات وتأكده من صحة بياناتها.

28. اجراء مطابقة ثنائية للمركز المالي والفروع بشكل يومي.
29. الفصل بين مهام الموظفين وكذلك الفصل بين مهام اللجان المختصة تحقيقا لمبدأ الشفافية المهنية والحوكمة المؤسساتية للتقليل من فرص تحقق عمليات التلاعب / الاحتيال / الاختلاس / التزوير.
30. وجود نماذج موحدة في تنفيذ العمليات المصرفية لدى البنك تضمن عدم التزوير والاحتيال والتلاعب من قبل العملاء.
31. الحفظ الامين للمستندات والشيكات البنكية والحوافظ اليومية والتقارير والبيانات المالية داخل خزائن ضد الحريق وبرقابة ثنائية.
32. زيارة العميل قبل المنح للاطلاع على الاوضاع والمركز المالي ومدى توافقه مع البيانات المالية المقدمة من طرفه, والتأكد من صحة ودقة البيانات الشخصية المقدمة من العميل.
33. تعزيز الفاكسات الواردة بمكالمات هاتفية قبل تنفيذ تعليمات العميل وتثبيت هذا التعزيز على نفس الطلب.
34. التحقق من مستندات العميل لدى فتح الحساب.
35. تحويل أثر وقوع حدث احتيال أو تزوير لطرف ثالث وذلك عن طريق عقد اتفاقيات مع جهات خارجية مثل (شركات التأمين) أو تضمينها من ضمن العقود الموقعة معهم.
36. استخدام أحدث التقنيات وذلك بأستخدام آلات عد نقد حديثة لكشف تزوير العملة.

أحد عشر : عرض خطة العمل للمصادقة عليها:

يتم مراجعة وعرض خطة وآليات العمل لمعرفة مدى كفاءتها وتحقيقها لاهدافها وتطويرها تبعا للتطور المصرفي بحيث يتم المصادقة عليها من قبل لجنة المجلس المختصة ، إلا في حال حدوث أي حدث طارئ يتم إجراء تعديل عليها لعلاج الثغرات فورا .

ملحق رقم (5) **محتويات البرنامج التدريبي**

1. المسؤوليات والالتزامات التي يفرضها القانون والتعليمات على البنك ومن ثم كافة موظفيه.
2. العقوبات الناتجة عن مخالفة تعليمات مكافحة غسل الاموال و تمويل الارهاب .
3. دور موظفي البنك في حمايته من الانخراط في أية خروقات أو انتهاكات للقانون والتعليمات.
4. الأساليب والطرق المستخدمة في غسل الأموال وتمويل الارهاب.
5. سياسة واجراءات البنك في مكافحة غسيل الاموال وتمويل الارهاب، والتعليمات ذات العلاقة.
6. سياسة اعرف عميلك.
7. مؤشرات الاشتباه .
8. اجراءات تقديم التقارير الداخلية (الابلاغ الداخلي).
9. آلية التعامل مع المشتبه بهم وفق التعليمات.
10. متطلبات التأكد من الهوية .

ملحق رقم (6) متطلبات الاحتفاظ بالتسجيلات / السجلات

1. يختلف تاريخ حساب بدء فترة الاحتفاظ بالمستندات والسجلات حسب أنواعها وفقا لما يأتي:
   1.1. سجلات ومستندات العملاء والمستفدين الحقيقين :-

   يتم الاحتفاظ بها لمدة لا تقل عن عشر سنوات من تاريخ اقفال الحساب ، أو من تاريخ انتهاء العملية بالنسبة للعمليات التي يتم تنفيذها لعملاء ليست لديهم حسابات.

   1.2. السجلات والمستندات المتعلقة بالعمليات التي تتم مع العملاء :-

   يتم الاحتفاظ بها لمدة لا تقل عن عشر سنوات من تاريخ اقفال الحساب، أو من تاريخ انتهاء العملية بالنسبة للعمليات التي يتم تنفيذها لعملاء ليست لديهم حسابات.

   1.3. السجلات والمستندات الاخرى: يراعى أن يتم الاحتفاظ لمدة عشر سنوات على الأقل بكل مما يأتي:
      1.3.1. تقارير العمليات غير العادية وذلك من تاريخ صدور التقرير.
      1.3.2. السجلات الخاصة بالعمليات المشتبه فيها التي تم إرسالها إلى وحدة مكافحة غسل الأموال وتمويل الارهاب وذلك من تاريخ إرسالها أوإلى حين صدور قرار أوحكم نهائى فى شأن العملية أيهما أطول
      1.3.3. سجلات ومستندات تقارير الاشتباه التي تم اتخاذ قرار بحفظها من قبل المدير المسؤول عن مكافحة غسل الأموال وتمويل الارهاب وذلك من تاريخ اتخاذ القرار بحفظها.
      1.3.4. السجلات الخاصة بالبرامج التدريبية ، وذلك من تاريخ انتهاء البرنامج التدريبي.

2. اصول جميع وثائق المعاملات سواء كانت محلية أو خارجية، لمدة لا تقل عن عشر سنوات من تاريخ الشروع او انتهاء المعاملة المالية بغض النظر عن بقاء أو انتهاء علاقة العمل على ان لا تقل مدة الاحتفاظ بالسجلات وملفات العملاء عن خمس سنوات من تاريخ اغلاق الحساب وتتضمن بصفة خاصة ما يلي:
   2.1. صور هويات أطراف المعاملة/ العملية.
   2.2. طبيعة وتاريخ المعاملة.
   2.3. نوع وحجم مبلغ المعاملة.
   2.4. مصدر الاموال.
   2.5. الاشكال والنماذج، الاوامر، التعليمات المستخدمة في المعاملة (سحب، ايداع، تحويل، شيك، ..الخ) .
   2.6. مقصد أو وجهة الاموال.
   2.7. نوع ورقم الحساب المتعلق بالمعاملة.

3. الوثائق والمستندات المتعلقة بفتح الحسابات للأشخاص الطبيعيين والاعتباريين، لمدة لا تقل عن 10 سنوات، مثل:
   3.1. شهادات التسجيل.
   3.2. نموذج/ طلب فتح الحساب.
   3.3. مستندات اثبات الشخصية (بطاقة هوية- جواز سفر- رخصة قيادة- وغيرها).
   3.4. صورالمراسلات ذات الصلة بعلاقة العمل.
   3.5. اي تقييم للمخاطر تم اجراؤه .
   3.6. اية فحوصات تم اجراؤها للتعرف على هوية العميل والغرض من المعاملات.

4. الوثائق والسجلات المتعلقة بأي معاملة يتم تنفيذها للعملاء الذين لا يملكون أي حساب لدى البنك (العملاء العرضيون) لمدة عشر سنوات على الأقل من تاريخ تنفيذ المعاملة.
5. السجلات والتقارير الخاصة بالعمليات غير العادية لمدة عشر سنوات على الاقل من تاريخ صدور التقرير بها.
6. السجلات والوثائق الخاصة بالعمليات المشتبه بها ونتائج تحليل المعاملات المشبوهة لمدة عشر سنوات على الأقل من تاريخ ارسالها لوحدة المتابعة المالية أو الى حين صدور حكم نهائي في شأن العملية في حال وجود قضايا تحقيقية أو صدور قرار نهائي من الجهة الرقابية ذات العلاقة، أيهما أطول.
7. المستندات والبيانات والمعلومات المتعلقة بإجراءات العناية الواجبة تجاه العميل لمدة لا تقل عن عشر سنوات.
8. مستندات نتائج الفحوصات والتحقيقات بالتنبيهات الخاصة من نظام مراقبة الحركات المالية والمطابقة على قوائم الحظر والتجميدوفق قوائم الحظر والتجميد واغلاقها لمدة عشر سنوات على الأقل من تاريخ انتهاء علاقة العمل مع العميل وقد تمتد في حال وجود قضايا تحفقيقية لحين انتهاء هذه القضايا
9. السجلات الخاصة بالبرامج التدريبية لمدة لا تقل عن 10 سنوات على الاقل، على أن تشتمل على بيانات كافة البرامج التي يحصل عليها الموظفون بالبنك في مجال مكافحة غسل الأموال، تمويل الإرهاب، مثل:
    9.1. أسم الموظف / المتدرب.
    9.2. القسم/ الإدارة التي يعمل بها.
    9.3. تاريخ / فترة التدريب.
    9.4. مدة التدريب.
    9.5. الجهة المنفذة/ المزودة للتدريب (داخلياً / خارجياً).
    9.6. محتوى البرنامج التدريبي/ موضوعات التدريب.
    9.7. موقع/ مكان التدريب.
    9.8. التقييمات المتعلقة بالتدريب.
10. الاحتفاظ بكافة السجلات والمستندات والتقارير بطريقة آمنة ، والاحتفاظ بنسخ احتياطية منها فى مكان آخر، وأن تتسم طريقة الحفظ بسهولة وسرعة استرجاع السجلات والمستندات المحتفظ بها ، وأن يتم توفير أية بيانات أو معلومات يتم طلبها بشكل وافي ودون تأخير.