CITY DEVELOPMENTS LIMITED ANTI MONEY LAUNDERING POLICY

City Developments Limited is committed to upholding strong governance and responsible business practices. As part of this commitment, the Group maintains an Anti-Money Laundering, Counter-Financing of Terrorism and Counter-Proliferation Financing (AML/CFT/CPF) Policy that guides our approach in preventing money laundering activities, terrorism financing and proliferation financing activities.

The Policy takes reference from the *Urban Redevelopment Authority (URA) Guidelines for Developers on Prevention of Money Laundering, Proliferation Financing and Terrorism Financing.* Risk-based policies and procedures have been established to anticipate and prevent money laundering, terrorist financing and proliferation financing within our business.

To support effective implementation, the Group emphasizes a strong compliance culture. All employees are required to complete mandatory annual declarations and training to reinforce awareness and strengthen capabilities in recognizing and managing financial-crime risks.

These measures are supported by customer due diligence processes, ongoing monitoring, escalation procedures and staff awareness requirements The Group also maintains a **zero-tolerance position** towards non-compliance with laws and regulations and towards criminally dishonest acts such as fraud, corruption, bribery and extortion.

Through these measures, the Group seeks to safeguard the integrity of property transactions and contribute to a safe and trusted operating environment.

Extract of Policy:

Section	Requirement/Guidance
4.2	**Risk Analysis** 4.2.1 Before launching any project for sale, developers must take appropriate steps to identify, assess and understand the ML/PF/TF risks in relation to: a. their purchasers; b. the countries and jurisdictions which their purchasers are from or in; c. the countries and jurisdictions in which developers have operations; and d. their services, transactions, and delivery channels. 4.2.2 In performing the risk analysis, developers must consider all relevant risk factors for each project regulated under the HDCLA and SCPA, before determining the developer's overall risk level. Thereafter, developers must: a. document their risk analysis; b. implement risk mitigating measures that are commensurate with the overall risk level and size of the developer's business; c. keep their risk analysis up to date. For example, developers could consider reviewing their risk analysis once every 2 years, or when material trigger events occur, whichever is earlier. Material trigger events include, but are not limited to, acquisition of new customer segments etc; and

Section	Requirement/Guidance
	d. have appropriate mechanisms to provide their risk analysis to the Controller of Housing, as appointed under Section 3(1) of the HDCLA. 4.2.3 Developers may refer to the risk analysis template in the Guidelines to guide them in performing their risk analysis. 4.2.4 Developers should consider all the following when determining if the purchaser presents a high risk of ML or TF: a. whether the relevant person[1] is a resident of or originates from: i. a relevant country; ii. a foreign country that the FATF by a public statement, notice or directive published on its official website at https://www.fatfgafi.org/en/topics/high-risk-and-other-monitoredjurisdictions,html identifies as a foreign country subject to increased monitoring. As defined by FATF, these are countries that are actively working with FATF to address strategic deficiencies in their regimes to counter money laundering, terrorism financing and proliferation financing; or iii. a foreign country that the Controller has notified the developers to be a foreign country with inadequate measures to prevent ML, PF or TF; or b. whether the transaction with the purchaser is complex or unusually large or is part of an unusual pattern of transactions which have no apparent economic or visible lawful purpose[2]. c. whether the relevant person or any other person acting on behalf of the purchaser is suspected of, or at risk of, facilitating ML, PF or TF, as notified by the Controller or other relevant authorities.
5	5 **Programmes and Measures to Prevent Money Laundering, Proliferation Financing and Terrorism Financing** **5.1 Governance on prevention of ML/PF/TF** 5.1.1 The commitment, participation and authority of the developer is important to a sound risk management framework to prevent ML/PF/TF. Developers should ensure that their risk mitigating measures are adequate, robust, and effective. The successful implementation of a risk-based approach to AMLTF requires developers to have a good understanding of the ML/TF risks they are exposed to. 5.1.2 The ML/PF/TF risks are not static as criminals will modify their ML/PF/TF methods to avoid detection and overcome measures put in place to manage ML/PF/TF risks. To encourage proper governance and a culture of compliance to prevent ML/PF/TF, developers and the Senior Management in the developers (e.g. a

[1] "**Relevant Person**" means a Purchaser, a beneficial owner of a purchaser, a person on whose behalf a purchaser is acting or a beneficial owner of that person.

[2] Complex transactions include attempts to disguise the BO(s) involved in the transaction, use of unnecessarily complex transaction structures designed to obscure the true nature of the transaction or involving the use of multiple intermediaries for the transaction. Unusually large transactions could include a transaction priced at more than the usual or expected amount for a similar typical transaction. Transactions with no apparent economic or lawful purpose could include using trust and company service providers to set up a number of corporate structures in multiple jurisdictions for the transaction without any apparent purpose.

Section	Requirement/Guidance
	director, Chief Executive Officer) should: a. obtain sufficient information to form an accurate picture of the ML/PF/TF risks, including emerging or new ML/PF/TF risks; b. obtain sufficient and objective information to assess whether the developers' AMLTF controls are adequate and effective; c. obtain information on legal and regulatory developments and the impact these have on developers' frameworks to prevent ML/PF/TF; and d. ensure that processes are in place to escalate important decisions that directly impact the ability of developers to manage and mitigate ML/PF/TF risks, especially where controls are assessed to be inadequate or ineffective to prevent ML/PF/TF. 5.1.3 Developers must develop and implement policies, procedures and controls, which must be approved by their Senior Management[3], taking into consideration the ML, PF and TF risks and the size of their business. This is to manage and effectively mitigate the ML and TF risks identified or notified by the Controller in writing, . The IPPC should include the following areas: a. making appropriate compliance management arrangements, including the appointment of a compliance officer at the management level e.g. a director, Chief Executive Officer, Chief Financial Officer, of the developer; and b. applying adequate ML/PF/TF screening procedures when hiring employees. c. Scope and frequency of developer's training programme for its staff 5.1.4 For a developer that is a company incorporated in Singapore and has a branch or subsidiary, whether in Singapore or elsewhere, the developer must develop and implement a group-level programme to prevent ML, PF and TF. The programme must: a. be applicable to all the developer's branches and subsidiaries, whether in Singapore or elsewhere; b. include the measures mentioned in paragraphs 4.2.1 and 4.2.2; c. be appropriate to the business of the developer's branches and subsidiaries; d. be implemented effectively at the level of the developer's branches and subsidiaries; e. include policies and procedures for providing and sharing information required for the purposes of CDD measures and generally for the management of risks relating to ML, PF and TF; and f. include adequate safeguards on the confidentiality and use of information exchanged between the developer and its branches and subsidiaries. 5.1.5 If the developer has a branch or subsidiary in a country or territory outside Singapore that has laws for the prevention of ML, PF or TF that differ from those

[3] The policies, procedures and controls must be approved by the Senior Management of the developers. Developers may also seek approval from their Board of Directors for the policies, procedures and controls, depending on their internal company policy.

Section	Requirement/Guidance
	in Singapore a. the developer must require the management of that branch or subsidiary to apply the more stringent set of laws, to the extent that the law of the host country or territory permits; b. if that branch or subsidiary is unable to fully apply the more stringent set of laws, the developer must report this to the Controller and must, in lieu of paragraph (a), comply with the Controller's directions. **5.2 AMLTF Governance** 5.2.1 Developers must have an ongoing programme to train employees on their IPPC. Examples include: a. roles and responsibilities of developers in combating ML/PF/TF, and in particular, CDD measures, and detecting and reporting of suspicious transactions; and b. internal policies, procedures and controlsto prevent ML/PF/TF. 5.2.2 The scope and frequency of training should be tailored to the specific risks faced by the developer and pitched according to the job functions, responsibilities and experience of the employees and officers. 5.2.3 Employees should have a good understanding of the MLPF/TF risks inherent in the developer's business. **5.3 Audit Function** 5.3.1 Developers must have an independent audit function to test the policies, procedures and controls as mentioned in paragraph 5.1.3, monitor the implementation and enhance the policies, procedures and controls if necessary.
6	**Customer Due Diligence ("CDD")** **6.1 What is CDD** 6.1.1 CDD refers to the process of identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. 6.1.2 There are three levels of customer due diligence - CDD, enhanced CDD and simplified CDD, to be applied to different levels of ML/PF/TF risk. 6.2 **When to perform CDD** 6.2.1 Developers are required to perform CDD in any of the following circumstances: a. before granting to a purchaser an option to purchase a unit, or before accepting any sum of money (including any booking fee) from a purchaser in relation to the intended purchase, whichever is earlier; b. when a purchaser intends to assign or has assigned to an assignee purchaser all the purchaser's rights, title and interest, under the Sale and Purchase

Section	Requirement/Guidance
	Agreement (S&PA) made between the purchaser and the developer, and when the developer receives written notice from the assignee purchaser requiring the developer to enter into a new S&PA with the assignee purchaser; c. when the developer has reasons to suspect that a purchaser is engaging in ML/PF/TF; d. when the developer has reason to doubt the veracity or adequacy of information obtained from earlier CDD measures about the same purchaser. 6.2.2 Developers can also refer to an indicative list of suspicious real estate transactions to look out for during the transactions with purchasers at https://www.police.gov.sg/-/media/SPF/Advisories/STRO/Red-Flag-Indicators-for-Developers-Real-Estate-Agents-and-Salespersons.pdf. 6.3 **How to perform CDD** 6.3.1 Developers must perform the following CDD measures in relation to every purchaser: a. ascertain the identity of the purchaser and obtain the purchaser's identifying information. Please refer to the list of identifying information in Forms A1 to A3. Developers should take reasonable measures to obtain and verify information on the purchaser's current and previous nationalities as well as identities, particularly if the ML/PF/TF risk of the purchaser is determined to be higher; b. where the purchaser is an entity or legal arrangement: i. obtain the documents that constitute, regulate and bind the purchaser[4]; ii. ascertain the identity of every individual holding a senior management office in the purchaser and obtain the individual's identifying information; c. understand and obtain information about the purchaser's purpose for purchasing a unit in a building project undertaken by that developer. d. ascertain whether the purchaser is acting on behalf of any other person (called P), and if so: i) obtain appropriate documentary evidence (such as an authorisation letter or power of attorney) to verify that the purchaser is authorised to act on behalf of P; ii) if P is a natural person, perform the CDD measures in sub-paragraphs (a) and (c) in relation to P(as if the references to a purchaser in those sub-paragraphs are references to; and if P is an entity or a legal arrangement, perform the CDD measures specified under paragraphs 6.3.1(a), (b) and (c) and 6.3.2 in relation to P (as if the

[4] In the case of a body corporate, the constitution, or the memorandum and articles of association, of the body corporate. In the case of a partnership or limited partnership, the partnership deed or agreement. In the case of an express trust, the trust deed of the trust. In the case of a society or an unincorporated association, the rules of the society or unincorporated association. In the case of any other entity or legal arrangement, the instrument or document that constitutes or establishes the entity or legal arrangement.

Section	Requirement/Guidance
	references to a purchaser in those sub-paragraphs are references to P). e. take reasonable measures to determine whether the purchaser or a natural person on whose behalf the purchaser is acting, is a politically exposed person or a family member or close associate of a politically exposed person. 6.3.2 For every purchaser or every person that the purchaser is acting on behalf, that is an entity or a legal arrangement, developers must: a. determine whether the entity or legal arrangement has any BO; b. take reasonable measures to ascertain the identity and obtain the identifying information of each BO of the entity or legal arrangement, if any; c. understand the nature of the business of the entity or legal arrangement; d. understand the ownership and control structure of the business of the entity or legal arrangement. Please refer to the CDD checklist in Annexure 2 for details on how to perform the CDD for purchases by an entity or a legal arrangement. 6.3.3 Developers need not ascertain the identity and obtain the identifying information of each BO of an entity is: a. an entity listed on the Singapore Exchange and is subject to disclosure requirements by the Singapore Exchange; b. a financial institution that is listed in Appendix 1 of the direction known as MAS Notice 626 issued by the Monetary Authority of Singapore; or c. a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with requirements for the prevention of ML and TF, consistent with standards set by the FATF. 6.3.4 Developers must record the basis for determining that the purchaser is an entity specified in paragraphs 6.3.3(a), (b) and (c). 6.3.5 For a person purporting to act on behalf of the purchaser, developers must: a. ascertain and obtain the identifying information of the person; b. ascertain whether the person is authorised to act on behalf of the purchaser, including by obtaining the appropriate evidence in writing of the authorization and appointment of the person by the purchaser to act on the purchaser's behalf. Developers may refer to the CDD checklist in Annexure 2 for details on how to perform the CDD. 6.3.6 Developers should screen all the relevant persons and persons acting on behalf of the purchaser against these lists and sources of information: a. Ministry of Home Affairs ("MHA")'s website on the Inter-Ministry Committee on Terrorist Designation ("IMC-TD") for information on terrorist designation and

Section	Requirement/Guidance
	requirements for countering the financing of terrorism; https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism b. First Schedule of the TSOFA https://sso.agc.gov.sg/Act/TSFA2002; c. Regulations under the United Nations Act 2001 (“UN Act”) available in MAS’ website https://www.mas.gov.sg/regulations-and-financial-stability/anti-money-laundering-countering-the-financing-of-terrorism-and-targeted-financial-sanctions/targetded-financial-sanctions/lists-of-designated-individuals-and-entities.aspx; d. list(s) provided by the Controller or other relevant authorities. In addition, developers may screen the relevant persons against public sources of information, such as websites or third party screening database. 6.3.7 Developers should subscribe to MAS’ website (by selecting “Anti-Money Laundering" under "Regulation Focus Areas”) through which they would be able to be kept updated on the latest designations by the United Nations Security Council, and other relevant updates to Singapore’s frameworks to prevent proliferation financing or terrorism financing. 6.3.8 When assessing adverse news alerts, developers should take into consideration the relevant person’s current and previous nationality and/or identity. Developers should not dismiss such screening alerts solely based on the relevant person’s current nationality or identity. Additional due diligence should be performed e.g. adverse media searches in native languages of countries known to be associated with the relevant person. 6.3.9 Where screening of the relevant person and person acting on behalf of the purchaser results in a positive hit against sanctions lists and lists as informed by the Controller or other relevant authorities, developers must: a. not grant an option to purchase any unit to the purchaser, accept any money (including booking fee) from or on behalf of the purchaser, or enter into a S&PA with the purchaser or assignee purchaser for a unit b. file a suspicious transaction report via the Suspicious Transaction Reporting Office Online Notices and Reporting platform (SONAR) at http://www.police.gov.sg/sonar c. cease all dealings with the designated persons and entities and where applicable, freeze without prior delay and prior notice, the funds or assets, including any purchase price paid and not refund any part of it, pending further instructions from STRO and/or relevant law enforcement authorities 6.4 **Failure to Satisfactorily Perform or Complete CDD Measures** 6.4.1 Developers may choose not to perform or not to complete the required CDD measures if they have reasons to: a. suspect that the transaction with or intended with the purchaser involves ML/TF; and

Section	Requirement/Guidance
	b. believe that performing the CDD measures will tip off the purchaser or any other person associated with the purchaser. 6.4.2 Developers are deemed to be unable to complete the CDD if: a. they are unable to obtain, or to verify, any information required as part of those CDD measures; or b. they do not receive a satisfactory response to any inquiry they make in relation to any information required as part of those CDD measures. 6.4.3 In the situations highlighted under paragraphs 6.4.1 and 6.4.2, developers must: a. not grant an option to purchase any unit to the purchaser, accept any money (including booking fee) from the purchaser, or enter into a S&PA for a unit with the purchaser or assignee purchaser; b. determine whether to file a STR; and c. record the basis of the determination under sub-paragraph (b).
7	7 **Enhanced Customer Due Diligence (“ECDD”)** **7.1 What is ECDD** 7.1.1 ECDD refers to the process where a higher level of CDD is applied due to higher ML/PF/TF risk of the customer or transaction. This is performed in addition to the CDD measures in paragraph 6. 7.2 **When to perform ECDD** 7.2.1 Developers are required to perform ECDD in any of the following circumstances: a. the relevant person in any transaction is: i. a foreign PEP, a family member or a close associate of a foreign PEP; or ii. is a resident of or originates from a relevant country; or iii. is a person that the Controller or other relevant authorities have notified the developer to be a person who presents a higher risk of ML, PF or TF; b. developers have assessed under paragraph 4.2 that the relevant person (including a domestic or international organisation PEP, family member or close associate of a domestic or international organisation PEP) may present a higher risk of ML or TF. 7.3 **Requirements of ECDD** 7.3.1 Where developers are required to perform ECDD, developers must perform the following measures in addition to the CDD requirements in paragraph 6: a. obtain prior and special approval from a person holding a senior managerial or executive position in the developer before granting an Option to Purchase (OTP) to a purchaser, or before accepting any sum of money (including any

Section	Requirement/Guidance
	booking fee) from a purchaser, or before entering into the S&PA with the purchaser or assignee purchaser; b. take reasonable measures to establish the income level, source of wealth (SoW) and source of funds (SoF)[5] of the relevant person; c. ascertain the identity of the person P on whose behalf the purchaser is acting and obtain P's identifying information, where the developer suspects that the purchaser is trying to conceal the identity of the person P; d. conduct enhanced ongoing monitoring of the transactions entered into with the purchaser. This is to identify suspicious transactions, including transactions or patterns of transactions which are inconsistent with the purchaser's profile. e. Take all reasonable measures as are appropriate to the risks of ML, PF or TF in relation to the relevant person 7.3.2 To establish the SoW and SoF, developers should document and make a reasonable assessment of the purchaser's representations by doing the following, in addition to obtaining the information from the purchaser's declarations: a. corroborate the information on SoW and SoF against documentary evidence or public information sources such as commercial databases, audited accounts, salary details, bank statements or other public information sources etc; Where independent documents or sources are not readily available, developers should assess whether residual risk of uncorroborated wealth is acceptable or additional risk mitigation measures would be necessary; b. conduct additional triangulation checks against a few sources to ensure robustness of assessment. For example, for a purchaser whose declared SoW was from his employment as a senior management of a Middle East global bank 10 years ago, developers should corroborate the purchaser's net worth by verifying his global position through online searches, obtaining salary benchmarks of finance professionals' salary in Middle East; c. exercise reasonable judgment in determining which documents and/or information are critical for SoW corroboration. E.g. Focus on corroborating the more material or higher risk SoW (such as SoW from higher risk countries or higher risk industries). Documents from many years ago may no longer be easily available and not be of high relevance to the customer's SoW. 7.3.3 Examples of information that developers can use to corroborate individuals' SOW/SOF: d. Salaries and savings: Salary slips, tax returns, bank statements showing the salary that has been credited;

[5] "**Source of Wealth**" (SoW) generally refers to the origin of the customer's and BO's entire body of wealth (i.e. total assets). Examples of appropriate means of establishing SoW are from evidence of title, copies of trust deeds, audited accounts, salary details, tax returns and bank statements. "**Source of Funds**" (SoF) refers to the origin of the particular funds or other assets which are the subject of the transactions. Examples of appropriate means of establishing SoF are from salary payments or business income.

Section	Requirement/Guidance
	e. Gift/inheritance/windfall: Bank statements/documents showing the payouts/transfers, will (for inheritance). Developers should establish the relationship between the asset contributor and the purchaser by reasonable means – such as obtaining birth certificate (if available) or address proof. Developers should also pay closer scrutiny to the legitimacy and reasonableness of the gift, especially if it is from unrelated parties. This could be done through obtaining independent information to verify a gifting transaction, and assessing the plausibility of the asset contributor's financial ability to provide as well as reasons for providing the gift. f. Business profits over the years: Audited financial statements showing the profits and dividend payments and the individual's ownership of the company. Information from company registers (e.g. ACRA's database) to corroborate the individual's ownership in the company, or changes in ownership. Unaudited management accounts should only be considered as an alternative. If used, developers should conduct additional triangulation checks against independent sources to assess the reliability of such unaudited financial information. g. Investment gains over the years: Independent documents evidencing the ownership of the shares, sale of shares, and dividend income. For SoW derived from dividend income, developers should independently establish the customer's shareholdings in the business, to assess the proportion of dividend income earned. If dividend income spans across many years, developers should seek to obtain several years' worth of financial statements, instead of using a couple of financial statements to extrapolate. Where financial statements are unavailable, additional independent benchmarks should be used to justify any assumption. h. Being a political office holder over the years (e.g. a foreign PEP): Reliable public information showing the individual's political position (e.g. Media articles from reliable media outlets stating the individual's position, government websites with information on the PEP). 7.3.4 Where the legitimacy of the relevant person's SoW and SoF cannot be reasonably ascertained, developers should: a. not grant an OTP or accept any sum of money (including booking fee) from an intending purchaser; or b. not enter into a new S&PA with the assignee purchaser for sub-sales; and c. determine whether to lodge a STR. 7.4 **How to perform ECDD** 7.4.1 Developers must implement appropriate policies, controls and procedures to determine whether the circumstances mentioned in paragraph 7.2 exist. For example, developers could consider increasing the frequency of their checks.

Section	Requirement/Guidance
	7.4.2 Developers can adopt the following checks, depending on their risk assessment: a. use the internet and media as sources for determining, verifying and monitoring information; b. access commercial screening databases to help identify the relevant person and to check against adverse news reports; c. refer to the FATF guidance paper on dealing with PEPs.
8	8 **Simplified Customer Due Diligence (“SCDD”)** **8.1 When to Perform SCDD** 8.1.1 Developers may, instead of performing the standard CDD measures in paragraph 6, perform SCDD measures if it is deemed that SCDD measures are adequate to effectively ascertain the identity of the purchaser or beneficial owner of the purchaser, or any person who is acting on behalf of the purchaser, in any particular transaction. 8.2 **Requirements of SCDD** 8.2.1 SCDD measures can only be performed if all the following conditions are met: a. developers have assessed the risk of ML, PF and TF in relation to the purchaser to be low; b. the SCDD measures are commensurate with the level of the risk of the relevant person engaging in ML, PF and TF, as identified by the developers; and c. none of the circumstances mentioned in paragraph 7 requiring ECDD measures exists. 8.3 **How to perform SCDD** 8.3.1 Developers must record the details of the risk assessment that forms the basis for the decision and the SCDD measures carried out.
9	9 **Customer Due Diligence (CDD) on Existing Purchasers** 9.1 For existing purchasers with whom developers have entered into a transaction before the implementation of the prevention of ML/PF/TF requirements, developers must perform CDD, ECDD and SCDD measures in relation to any existing purchaser, taking into account: a. when CDD, ECDD or SCDD measures (if any) were last applied to that purchaser; and b. the adequacy of information already obtained by the developer in relation to that purchaser. 9.2 Developers may use information previously obtained from CDD, ECDD or

Section	Requirement/Guidance
	SCDD measures performed in relation to the same purchaser unless developers have doubts about the veracity or adequacy of the information, or whether the information is up-to-date. For existing purchasers, developers should conduct CDD, ECDD or SCDD before issuing the notice of payment for temporary occupation permit (TOP) or completion of sale, whichever is applicable. 9.3 If the existing purchasers originated from or are residents of high-risk countries or jurisdictions subject to a call for action by FATF (“FATF black list”), developers should perform enhanced ongoing monitoring of the transaction which could include more frequent checks on the source of wealth and funds, payment patterns etc.
10	10 **Performance of CDD Measures by Third Parties** 10.1 Developers may rely on a third party to perform the CDD measures which developers are required to perform, if the following requirements are met: a. developers are satisfied that the third party it intends to rely on: i. is subject to and supervised for compliance with requirements for the prevention of ML, PF and TF consistent with standards set by the FATF; ii. has adequate measures in place to comply with the FATF requirements; and iii. is willing and able to provide, without delay, on the developer’s request, any document acquired by the third party as a result of the CDD, ECDD or SCDD measures performed for the developer. b. the third party is not precluded from acting as such by the Controller; c. developers take appropriate steps to identify, assess and understand the risks of ML, PF and TF in the foreign countries that the third party also conducts its business in, if applicable. 10.2 Where a developer decides to rely on a third party to carry out CDD, ECDD or SCDD measures which will be based on the third party’s own prevention of ML/PF/TF rules and processes, the developer must: a. document the basis for the developer’s opinion in paragraph 10.1a; and b. obtain from the third party without delay all documents acquired as a result of the CDD, ECDD or SCDD measures performed by the third party; c. be ultimately responsible for compliance with the obligations to perform CDD, ECDD or SCDD measures and keep records as required under the Acts and Rules. 10.3 Developers are not allowed to rely on a third party to conduct ongoing monitoring (see Para 11), as the CDD measures are conducted based on the third party’s own prevention of ML/PF/TF rules and processes and developers would not be able to have adequate control, timely information and ability to mitigate the risks arising from unusual/suspicious transactions during the ongoing monitoring process.

Section	Requirement/Guidance
11	11 **Ongoing Monitoring of Transactions** 11.1 Developers must, before issuing the notice of payment for TOP and for completion of sale, review the adequacy of the information and documents obtained as a result of the CDD,ECDD or SCDD measures. This is to ascertain whether the transactions carried out by the purchasers are consistent with the developers' knowledge of the purchaser, the purchaser's income and risk profile and the purchaser's source(s) of funds, particularly in cases where there is a higher risk of ML, PF or TF.
12	12 **Reporting of Suspicious Transactions** **12.1 Submitting a Suspicious Transaction Report** 12.1.1 If there are suspicions that ML/PF/TF activities are committed, developers are required to file a STR at https://www.police.gov.sg/sonar 12.1.2 The filing of an STR should be done as soon as possible, which should be within 5 business days after suspicion was first established, and within 15 business days of the case being referred by the developer's staff, unless the circumstances are exceptional or extraordinary. In cases where the relevant person or person acting on behalf of the purchaser is a sanctioned party, developers should file the STRs immediately, no later than 1 business day after suspicion was first established. 12.1.3 The STR must be filed electronically via SONAR. Developers may refer to the instructions on the SONAR website at https://www.police.gov.sg/sonar on how tofile a STR.
13	13 **Record Keeping** 13.1 Developers are required to keep the following documents and information (including any analysis performed) relating to a person whom CDD or ECDD or SCDD measures have been performed, for 5 years after the expiry or cancellation of the OTP, or the termination or annulment of the S&PA, or the legal completion of the sale and purchase of the property, whichever is applicable: a. OTP; b. S&PA; c. c. Form 3; d. Prescribed form to notify purchasers of the information/documents required for CDD checks; and e. Records of CDD, ECDD or SCDD conducted.

Section	Requirement/Guidance
14	14 **Additional Measures Relating to Targeted Financial Sanctions** 14.1 Before granting an OTP to a purchaser or before entering into a S&PA with a purchaser or assignee purchaser, developers must take reasonable measures to assess whether the relevant person or any person acting on behalf of the purchaser is: a. a terrorist or terrorist entity under the TSOFA; b. a designated person as defined in any regulations made under the UN Act; or c. a person suspected of, or at risk of, facilitating ML, PF or TF who is specified by the Controller in any written notice issued by the Controller 14.2 If a developer has reason to suspect that the circumstances in paragraphs 14.1(a), (b) or (c) exist, the developer must: a. not grant an option to purchase any unit to the purchaser, accept any money (including booking fee) from the purchaser, or enter into a S&PA for a unit with the purchaser; b. file a STR.
15	15 **Identifying risks from new technologies** 15.1 Developers must identify and assess the ML/PF/TF risks that may arise in relation to: a. the development of any new service or new business practice (including any new delivery mechanism for any new or existing service); and b. the use of any new or developing technology for any new or existing service.
16	16 **Managing and mitigating risks from new technologies** 16.1 Before offering any new service, starting any new business practice, using any new or developing technology, developers must assess the ML/TF risks that may arise in relation to the offering of that service, the starting of that business practice or the use of that technology. Subsequently, developers must take appropriate measures to manage and mitigate such risks.

Last updated: 4 Dec 2025