**KEBIJAKAN DAN PROSEDUR ANTI PENCUCIAN UANG DAN PENCEGAHAN PENDANAAN TERORISME (APU/PPT)**

**PT Digital Asset Vault**

**Tujuan**

Kebijakan dan prosedur internal ini disusun untuk memastikan bahwa PT Digital Asset Vault (selanjutnya disebut “Perusahaan”) mematuhi semua ketentuan Anti Pencucian Uang (APU) dan Pencegahan Pendanaan Terorisme (PPT) yang berlaku di Indonesia. Dokumen ini bertujuan untuk mencegah Perusahaan digunakan sebagai sarana pencucian uang atau pendanaan terorisme, melindungi integritas sistem keuangan, serta memenuhi persyaratan regulator domestik dan standar internasional (termasuk FATF Travel Rule dan ketentuan MiCA di Uni Eropa jika relevan)​file-b2ykmf7wrqem7zpyx9hqtm. Prosedur ini juga diselaraskan dengan standar Binance selaku platform P2P tempat Perusahaan beroperasi, termasuk menjawab kewajiban dalam kuesioner APU/PPT Binance​file-b2ykmf7wrqem7zpyx9hqtm. Dengan demikian, Perusahaan berkomitmen menerapkan pendekatan berbasis risiko untuk mengenali nasabah dan transaksi, mendeteksi serta melaporkan aktivitas mencurigakan, dan mematuhi semua kewajiban hukum terkait APU/PPT.

**Dasar Hukum**

Kebijakan ini dibuat berdasarkan kerangka hukum Indonesia dan standar global yang berlaku, antara lain:

* **Undang-Undang No. 8 Tahun 2010** tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang​file-b2ykmf7wrqem7zpyx9hqtm.
* **Undang-Undang No. 9 Tahun 2013** tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme​file-b2ykmf7wrqem7zpyx9hqtm.
* **POJK No. 12/POJK.01/2017** (Otoritas Jasa Keuangan) tentang Penerapan Program APU dan PPT di Sektor Jasa Keuangan​file-b2ykmf7wrqem7zpyx9hqtm, beserta perubahannya (POJK No. 23/POJK.01/2019).
* **Peraturan BAPPEBTI No. 6 Tahun 2019** tentang Penerapan Program APU dan PPT terkait Penyelenggaraan Pasar Fisik Komoditi di Bursa Berjangka​file-b2ykmf7wrqem7zpyx9hqtm.
* **Peraturan BAPPEBTI No. 8 Tahun 2021** tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto di Bursa Berjangka​file-b2ykmf7wrqem7zpyx9hqtm. *(Catatan: per Januari 2025, fungsi pengaturan dan pengawasan aset kripto dialihkan dari BAPPEBTI ke OJK sesuai amanat UU No.4/2023 (P2SK), sehingga Perusahaan akan menyesuaikan kepatuhan dengan regulasi OJK terbaru sebagaimana berlaku).*
* **Standar Internasional:** Rekomendasi FATF mengenai APU/PPT (termasuk Travel Rule FATF yang mewajibkan pertukaran informasi pengirim/penerima aset kripto) dan Regulasi Uni Eropa **MiCA** (Markets in Crypto-Assets Regulation) sebagai acuan praktik terbaik global​file-b2ykmf7wrqem7zpyx9hqtm.
* **Persyaratan Binance:** Panduan dan kebijakan APU/PPT Binance (misalnya *AML & CTF Questionnaire*, versi Nov 2024) yang relevan bagi merchant P2P Binance​file-b2ykmf7wrqem7zpyx9hqtm.

**Definisi**

**Tindak Pidana Pencucian Uang (TPPU):** Perbuatan menyembunyikan atau menyamarkan asal-usul hasil tindak pidana sehingga seolah-olah menjadi harta kekayaan yang sah. Definisi ini merujuk pada pengertian *Pencucian Uang* sesuai UU 8/2010, yakni segala perbuatan yang memenuhi unsur tindak pidana pencucian uang menurut undang-undang tersebut​file-b2ykmf7wrqem7zpyx9hqtm.

**Tindak Pidana Pendanaan Terorisme:** Segala perbuatan penyediaan, pengumpulan, pemberian, atau pemanfaatan dana, baik langsung maupun tidak langsung, dengan maksud digunakan untuk kegiatan terorisme atau untuk organisasi teroris. Definisi ini mengacu pada UU 9/2013 tentang Pendanaan Terorisme​file-b2ykmf7wrqem7zpyx9hqtm.

**APU/PPT:** Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme, mencakup upaya, program, dan prosedur untuk mencegah dan memberantas TPPU dan pendanaan terorisme​file-b2ykmf7wrqem7zpyx9hqtm.

**Perusahaan:** PT Digital Asset Vault, perseroan terbatas yang terdaftar di Indonesia dan beroperasi sebagai pedagang P2P aset kripto pada platform Binance​file-b2ykmf7wrqem7zpyx9hqtm.

**Nasabah/Pengguna Jasa:** Pihak (perorangan atau entitas) yang bertransaksi dengan Perusahaan. Dalam konteks P2P Binance, Nasabah diartikan sebagai mitra transaksi (pembeli atau penjual aset kripto) yang berinteraksi dengan Perusahaan melalui platform Binance​file-b2ykmf7wrqem7zpyx9hqtm.

**Beneficial Owner (BO):** Orang perseorangan yang secara langsung atau tidak langsung memiliki atau mengendalikan Nasabah, atau pihak yang menikmati manfaat akhir dari suatu hubungan bisnis. Termasuk di dalamnya pemilik sebenarnya dari suatu entitas (dengan kepemilikan >25% atau kontrol signifikan lainnya) atau individu yang bertindak atas nama pihak lain​file-b2ykmf7wrqem7zpyx9hqtm.

**Politically Exposed Person (PEP):** Orang yang tergolong berpengaruh secara politik, yakni individu yang menduduki posisi publik terkemuka (contoh: pejabat tinggi negara, pimpinan lembaga pemerintah, anggota keluarga dekat atau rekan dekat mereka). PEP berisiko lebih tinggi terkait pencucian uang karena potensi penyalahgunaan kekuasaan dan dana​file-b2ykmf7wrqem7zpyx9hqtm.

**Transaksi:** Segala kegiatan penempatan, transfer, pembayaran, penarikan, penukaran, atau perbuatan lainnya yang mengakibatkan perubahan kepemilikan atau pergerakan dana atau aset​file-b2ykmf7wrqem7zpyx9hqtm.

**Transaksi Keuangan Mencurigakan (TKM):** Transaksi yang memenuhi kriteria *mencurigakan* sebagaimana diatur UU 8/2010, antara lain: menyimpang dari profil atau kebiasaan Nasabah, diduga untuk menghindari pelaporan, melibatkan dana yang diduga hasil tindak pidana, atau transaksi yang diminta oleh PPATK untuk dilaporkan​file-b2ykmf7wrqem7zpyx9hqtm.

**Laporan Transaksi Keuangan Mencurigakan (LTKM):** Laporan yang wajib disampaikan oleh Perusahaan (sebagai Pihak Pelapor) kepada PPATK apabila menemukan Transaksi Keuangan Mencurigakan sesuai ketentuan. Laporan ini bersifat rahasia dan Nasabah tidak boleh diberitahu bahwa laporan telah dibuat​file-b2ykmf7wrqem7zpyx9hqtm.

**PPATK:** Pusat Pelaporan dan Analisis Transaksi Keuangan, lembaga intelijen keuangan Indonesia yang menerima laporan TKM, menganalisis, dan meneruskan ke penegak hukum​file-b2ykmf7wrqem7zpyx9hqtm.

**Travel Rule:** Aturan internasional (FATF Rekomendasi 16) yang mewajibkan penyedia jasa aset virtual (VASP), termasuk bursa kripto atau pihak yang memfasilitasi transfer aset kripto, untuk menyertakan dan berbagi informasi pengirim dan penerima dalam setiap transfer aset kripto antar institusi​file-b2ykmf7wrqem7zpyx9hqtm. Travel Rule umumnya diaplikasikan untuk transfer aset kripto ≥ USD 1.000 (atau setara) dan mengharuskan penyimpanan data tersebut minimal 5 tahun​file-b2ykmf7wrqem7zpyx9hqtm.

**MiCA:** *Markets in Crypto-Assets Regulation* – Regulasi Uni Eropa 2023 yang menetapkan kerangka perizinan dan kewajiban bagi penerbit dan penyedia layanan aset kripto di wilayah EU. Meskipun tidak berlaku langsung di Indonesia, prinsip-prinsip MiCA digunakan sebagai acuan *best practice*, terutama terkait transparansi, perlindungan nasabah, dan integritas pasar aset kripto​file-b2ykmf7wrqem7zpyx9hqtm.

**Tanggung Jawab dan Cakupan**

**Cakupan:** Kebijakan ini berlaku bagi seluruh kegiatan usaha Perusahaan, khususnya aktivitas sebagai merchant P2P Binance yang fokus pada jual beli aset kripto melalui platform Binance. Seluruh pegawai, manajemen, dan pihak terkait (termasuk Direksi dan Komisaris) wajib memahami dan mematuhi prosedur APU/PPT ini. Kebijakan mencakup interaksi Perusahaan dengan pengguna Binance (sebagai mitra transaksi), pengelolaan dana fiat yang diterima/dikirim melalui rekening bank Perusahaan, serta pengelolaan aset kripto pada dompet/platform yang digunakan Perusahaan​file-b2ykmf7wrqem7zpyx9hqtm.

**Dewan Direksi:** Direksi bertanggung jawab tertinggi atas kepatuhan APU/PPT di Perusahaan. Direksi wajib menyetujui dan meninjau kebijakan APU/PPT ini secara berkala (minimal setiap tahun)​file-b2ykmf7wrqem7zpyx9hqtm, memastikan tersedianya sumber daya yang memadai untuk pelaksanaan program APU/PPT, serta menetapkan budaya kepatuhan yang tinggi. Direksi juga menunjuk secara resmi Pejabat Kepatuhan/AML (AML Compliance Officer) yang kompeten (lihat bagian Penunjukan AML Officer). Setiap perubahan signifikan pada kebijakan harus disetujui Direksi.

**Manajemen Kepatuhan/AML Officer:** Pejabat yang bertanggung jawab atas penerapan harian program APU/PPT (sering disebut Officer APU/PPT atau MLRO). Tugas utamanya meliputi: koordinasi penerapan kebijakan ini, melakukan identifikasi dan evaluasi risiko, memastikan KYC/CDD dijalankan, memantau transaksi, menelaah dan menindaklanjuti indikasi transaksi mencurigakan, serta menyampaikan laporan ke PPATK tepat waktu​file-b2ykmf7wrqem7zpyx9hqtm. AML Officer juga menjadi kontak utama dengan regulator (PPATK, BAPPEBTI/OJK) dan dengan tim kepatuhan Binance bila diperlukan. Pejabat ini wajib memiliki akses langsung ke Direksi dan independensi dalam menjalankan fungsinya.

**Pegawai dan Pihak Terkait:** Setiap pegawai Perusahaan (termasuk karyawan operasional, administrasi, keuangan, IT, maupun agen/kontraktor yang terlibat) memiliki tanggung jawab untuk:

* Mematuhi prosedur APU/PPT dalam setiap aktivitas terkait pekerjaannya.
* Mengikuti pelatihan APU/PPT yang diwajibkan oleh Perusahaan.
* Mengenali dan melaporkan kepada AML Officer jika menemukan perilaku atau transaksi Nasabah yang tidak biasa atau mencurigakan.
* Menjaga kerahasiaan informasi terkait pemantauan dan pelaporan APU/PPT (tidak melakukan *tipping off* kepada Nasabah).

**Lingkup Kewajiban:** Prosedur internal APU/PPT ini mencakup: penilaian risiko, pelaksanaan KYC (Kenali Nasabah)/CDD/EDD, pemantauan transaksi, pelaporan transaksi mencurigakan dan/atau transaksi tunai tertentu (jika ada) kepada PPATK, penyimpanan catatan, pelatihan karyawan, audit internal kepatuhan, mekanisme pelaporan pelanggaran, serta sanksi internal atas pelanggaran kebijakan​file-b2ykmf7wrqem7zpyx9hqtm. Seluruh aspek tersebut didesain sesuai prinsip kehati-hatian dan proporsional dengan risiko Perusahaan.

Perusahaan juga memastikan tidak menjalin hubungan bisnis dengan “shell bank” atau institusi fiktif yang tidak memiliki kehadiran fisik atau lisensi yang sah​file-b2ykmf7wrqem7zpyx9hqtm. Setiap calon mitra atau institusi koresponden (jika relevan) harus melalui verifikasi kepatuhan.

**Mekanisme Layanan P2P Binance**

Sebagai pedagang P2P di Binance, Perusahaan memanfaatkan mekanisme escrow yang disediakan platform untuk menjamin keamanan transaksi. Pada setiap order jual/beli aset kripto, aset kripto milik penjual akan otomatis ditahan oleh Binance dalam deposit sementara (escrow) hingga pembeli mengirim dana fiat dan transaksi dikonfirmasi berhasil​[binance.com](https://www.binance.com/en/blog/all/how-does-binance-p2ps-escrow-service-work-421499824684900825#:~:text=An%20escrow%20service%20is%20an,giving%20traders%20peace%20of%20mind)​[binance.com](https://www.binance.com/en/blog/all/how-does-binance-p2ps-escrow-service-work-421499824684900825#:~:text=Once%20the%20buyer%20places%20an,successfully%20completed%20by%20both%20parties). Mekanisme escrow ini mencegah terjadinya penipuan atau wanprestasi, karena aset kripto hanya dilepaskan kepada pembeli setelah pembayaran terverifikasi.

Perusahaan hanya menggunakan rekening bank resmi atas nama perusahaan untuk menerima dan mengirim dana fiat dalam transaksi P2P. Perusahaan memastikan bahwa nama pemilik rekening bank pengirim atau penerima sesuai dengan nama Nasabah yang terdaftar pada platform Binance, sehingga mencegah penyalahgunaan rekening pihak ketiga. Transfer dari atau kepada rekening yang bukan atas nama Nasabah yang bertransaksi tidak diperbolehkan demi menjaga prinsip KYC dan mencegah praktik pencucian uang melalui rekening *nominee*​[binance.com](https://www.binance.com/en/support/faq/binance-p2p-user-transaction-policy-360041066751#:~:text=2,verified%20payment%20method%20has%20been). Perusahaan juga tidak menerima setoran tunai secara langsung maupun transfer di luar rekening bank yang terdaftar. Apabila terdeteksi pembayaran oleh pihak ketiga atau dana masuk yang tidak sesuai, transaksi tidak akan dilanjutkan dan dapat dilaporkan sebagai aktivitas mencurigakan untuk ditindaklanjuti.

Seluruh alur dana fiat dalam transaksi P2P dikendalikan dengan ketat dan terdokumentasi dengan jelas. Dengan prosedur di atas, layanan P2P yang disediakan Perusahaan tetap mematuhi persyaratan Binance serta standar APU/PPT internasional yang berlaku. Kebijakan seperti pelarangan transfer pihak ketiga sejalan dengan aturan Binance P2P dan rekomendasi FATF (misalnya penerapan prinsip *Travel Rule*) untuk mencegah penyalahgunaan platform. Perusahaan juga senantiasa mengikuti pembaruan kebijakan Binance P2P agar tidak ada celah yang dapat dimanfaatkan pelaku kejahatan finansial.

**Prosedur Penilaian Risiko**

Perusahaan menerapkan Pendekatan Berbasis Risiko (*Risk-Based Approach*) dalam program APU/PPT sesuai ketentuan regulator. Secara terperinci, langkah-langkah penilaian risiko adalah sebagai berikut​file-b2ykmf7wrqem7zpyx9hqtm:

**Identifikasi Risiko:** Perusahaan mengidentifikasi risiko-risiko pencucian uang dan pendanaan terorisme yang melekat pada kegiatan usahanya. Faktor risiko utama mencakup: profil dan perilaku Nasabah (misal: apakah termasuk PEP atau berdomisili di yurisdiksi berisiko tinggi; lihat Lampiran: Daftar Yurisdiksi Berisiko Tinggi), negara atau wilayah geografis asal/tujuan transaksi, produk/jasa yang ditawarkan (dalam hal ini perdagangan aset kripto P2P), kanal atau metode transaksi (platform digital Binance, transfer bank, dll.), serta volume dan frekuensi transaksi​file-b2ykmf7wrqem7zpyx9hqtm. Sebagai pedagang aset kripto, Perusahaan menyadari bahwa sektor aset virtual dikategorikan berisiko tinggi oleh banyak otoritas, sehingga mitigasi risiko harus lebih ketat​file-b2ykmf7wrqem7zpyx9hqtm.

**Penilaian dan Penentuan Tingkat Risiko:** Setelah identifikasi, AML Officer melakukan penilaian untuk mengukur tingkat risiko (rendah, menengah, atau tinggi) untuk setiap faktor dan setiap Nasabah. Perusahaan menggunakan kriteria terstruktur (misalnya skoring atau matriks risiko) untuk menilai profil Nasabah dan situasi transaksi. Kriteria evaluasi Nasabah antara lain: latar belakang dan pekerjaan Nasabah, tujuan penggunaan layanan Perusahaan, sumber dana yang akan digunakan, status PEP, negara asal, dan riwayat transaksi​file-b2ykmf7wrqem7zpyx9hqtm. Setiap Nasabah baru akan diberikan klasifikasi risiko awal (misal: risiko tinggi untuk PEP atau asal negara berisiko; risiko rendah untuk Nasabah domestik dengan profil sederhana). Hasil penilaian dicatat dalam Profil Risiko Nasabah (lihat Lampiran: Formulir Profil Nasabah).

**Mitigasi Risiko:** Berdasarkan tingkat risiko, Perusahaan menerapkan tingkat pengawasan dan upaya *due diligence* yang sesuai. Untuk Nasabah risiko rendah, dimungkinkan penerapan prosedur standar atau bahkan *Simplified Due Diligence* sesuai ketentuan (bila diizinkan oleh regulator) – misalnya persyaratan dokumentasi lebih terbatas namun tetap memenuhi minimum yang diatur UU. Untuk Nasabah risiko tinggi, Perusahaan akan menerapkan langkah-langkah *Enhanced Due Diligence* (EDD) (lihat bagian Kebijakan KYC/CDD/EDD) seperti verifikasi tambahan, permintaan dokumen sumber dana, atau persetujuan manajemen sebelum melanjutkan hubungan bisnis​file-b2ykmf7wrqem7zpyx9hqtm.

**Dokumentasi Risiko:** Semua proses identifikasi dan penilaian risiko didokumentasikan secara rapi. Perusahaan menyimpan Laporan Penilaian Risiko tertulis yang memuat metodologi, hasil penilaian, dan daftar risiko teridentifikasi. Dokumentasi ini akan diperlihatkan kepada otoritas pengawas jika diminta​file-b2ykmf7wrqem7zpyx9hqtm dan digunakan sebagai dasar penerapan kebijakan APU/PPT.

**Tinjauan dan Pembaruan:** Penilaian risiko Perusahaan akan ditinjau dan diperbarui secara berkala (minimal setiap 1 tahun) atau segera jika terjadi peristiwa tertentu yang mempengaruhi profil risiko. Misalnya, jika ada perubahan regulasi, perubahan profil jenis Nasabah, penambahan jenis layanan baru, atau adanya skema pencucian uang baru yang teridentifikasi di industri aset kripto. AML Officer bertanggung jawab memastikan Risk Assessment terbaru selalu tersedia. Pembaruan juga mempertimbangkan *National Risk Assessment* dari regulator Indonesia dan laporan risk assessment regional/global (misal FATF) agar sejalan dengan tren terbaru​file-b2ykmf7wrqem7zpyx9hqtm.

Dengan proses di atas, Perusahaan berusaha memastikan bahwa sumber daya dialokasikan secara tepat sesuai tingkat risiko, sehingga upaya pencegahan dapat difokuskan ke area yang paling rawan.

**Kebijakan KYC, CDD, dan EDD**

Perusahaan menerapkan kebijakan “Kenali Nasabah” (*Know Your Customer/KYC*) secara menyeluruh sebagai bagian dari Customer Due Diligence (CDD). Proses KYC/CDD dilakukan sebelum Perusahaan melakukan transaksi atau hubungan bisnis dengan Nasabah, serta secara berkelanjutan selama hubungan tersebut berlangsung​file-b2ykmf7wrqem7zpyx9hqtm. Berikut prinsip dan langkah kebijakan KYC/CDD/EDD:

**1. Proses Identifikasi dan Verifikasi Nasabah (CDD):**

*Pengumpulan Informasi Identitas:* Pada saat akan melakukan transaksi P2P dengan pihak lain, Perusahaan memastikan identitas calon lawan transaksi telah terverifikasi. Karena transaksi difasilitasi melalui platform Binance, Perusahaan hanya akan bertransaksi dengan pengguna Binance yang telah lulus verifikasi KYC Binance (minimal memenuhi persyaratan identifikasi level tertentu). Sebelum menerima transaksi, AML Officer/pegawai terkait memeriksa profil pengguna di platform (misal: status verifikasi “Terverifikasi” di Binance). Data yang dikumpulkan mencakup: nama lengkap sesuai identitas, tanggal lahir, kewarganegaraan, nomor identitas (KTP/Paspor), alamat, dan dokumen identitas yang diunggah. Apabila Perusahaan langsung menerima Nasabah (di luar platform), maka Nasabah wajib mengisi Formulir KYC (lihat Lampiran) disertai fotokopi identitas resmi dan foto diri (*selfie*) untuk keperluan verifikasi​file-b2ykmf7wrqem7zpyx9hqtm.

*Verifikasi Identitas:* Perusahaan memverifikasi keaslian data identitas Nasabah melalui dokumen resmi. Contohnya, mencocokkan nama dan NIK pada KTP dengan database Dukcapil atau layanan e-KYC, serta mengecek keaslian paspor. Selain itu, Perusahaan memverifikasi kecocokan nama pada rekening bank Nasabah yang digunakan untuk transaksi fiat dengan nama pada identitas. Transaksi hanya akan dilanjutkan jika nama pemilik rekening bank sesuai dengan nama Nasabah terdaftar, guna mencegah penyalahgunaan rekening pihak ketiga​file-b2ykmf7wrqem7zpyx9hqtm.

*Identifikasi Beneficial Owner:* Jika Nasabah merupakan korporasi atau diduga bertindak untuk pihak lain, Perusahaan wajib mengidentifikasi dan memverifikasi siapa Beneficial Owner sebenarnya. Perusahaan akan meminta dokumen pendirian perusahaan, struktur kepemilikan saham, serta data Ultimate Beneficial Owner (UBO) yang memiliki kendali >25%. Nasabah korporasi juga diminta melengkapi Formulir Pernyataan Beneficial Owner (jika berlaku) dan memberikan KTP Direksi/Pemilik. Beneficial Owner tersebut diperlakukan sebagai Nasabah perorangan yang harus lulus proses KYC (dikenali dan diverifikasi identitasnya)​file-b2ykmf7wrqem7zpyx9hqtm.

*Informasi Tambahan:* Perusahaan mengumpulkan informasi mengenai tujuan dan sifat hubungan bisnis yang diinginkan Nasabah. Misalnya: Nasabah menyatakan tujuan bertransaksi kripto (investasi pribadi, trading rutin, arbitrase, dll.) dan perkiraan volume transaksi. Informasi ini dicatat dalam profil Nasabah. Untuk Nasabah korporasi, data tentang bidang usaha, struktur kepengurusan, dan izin usaha (jika ada) juga dikumpulkan​file-b2ykmf7wrqem7zpyx9hqtm.

*Pemeriksaan PEP dan Sanksi:* Perusahaan melakukan screening terhadap calon Nasabah terhadap daftar PEP dan daftar sanksi terpublikasi (misal: daftar teroris atau individu terkena sanksi internasional/OFAC/UN). Alat screening bisa berupa pengecekan manual terhadap daftar yang disediakan pemerintah/OJK atau menggunakan tools screening otomatis. Jika calon Nasabah teridentifikasi sebagai PEP atau berada dalam daftar sanksi, AML Officer menandai Nasabah tersebut sebagai risiko tinggi dan menerapkan EDD (atau menolak hubungan bisnis jika berisiko melanggar sanksi). Nasabah juga diminta mengisi Formulir Deklarasi PEP untuk mengungkap status PEP atau bukan​file-b2ykmf7wrqem7zpyx9hqtm.

**2. Klasifikasi Risiko dan EDD (Enhanced Due Diligence):**

*Nasabah Berisiko Tinggi:* Untuk Nasabah dengan profil risiko tinggi (contoh: PEP, alamat negara berisiko tinggi, volume transaksi sangat besar, atau ada indikasi perilaku tidak biasa), Perusahaan menerapkan Enhanced Due Diligence (EDD). Langkah EDD meliputi persetujuan tambahan dari manajemen sebelum menerima Nasabah tersebut, pengumpulan dokumen ekstra seperti: bukti asal-usul kekayaan dan sumber dana (misal slip gaji, surat keterangan penghasilan, laporan rekening koran, dokumen penjualan aset, dll.), informasi bisnis atau pekerjaan secara terperinci, dan referensi bank jika perlu​file-b2ykmf7wrqem7zpyx9hqtm. Nasabah risiko tinggi juga diminta mengisi Formulir Pernyataan Sumber Dana yang menegaskan legalitas dan asal muasal dana yang akan digunakan. Setiap dokumen EDD diverifikasi keabsahannya (contoh: menghubungi institusi penerbit slip gaji untuk konfirmasi, jika relevan).

*Monitoring Ketat:* Nasabah berisiko tinggi akan dikenakan monitoring transaksi yang lebih intens (real-time atau review pasca-transaksi yang lebih mendalam setiap kali transaksi terjadi). Batasan limit transaksi bisa diterapkan lebih rendah, atau peninjauan manual oleh AML Officer sebelum transaksi dieksekusi​file-b2ykmf7wrqem7zpyx9hqtm.

*Kunjungan atau Wawancara:* Dalam kasus tertentu, Perusahaan dapat melakukan wawancara langsung dengan Nasabah berisiko tinggi untuk memahami profilnya, atau meminta pertemuan tatap muka/online *video call* untuk verifikasi tambahan​file-b2ykmf7wrqem7zpyx9hqtm.

*PEP:* Apabila Nasabah teridentifikasi sebagai PEP, selain langkah di atas, Perusahaan melakukan EDD khusus PEP, antara lain mencari tahu latar belakang jabatan publiknya, masa jabatannya, dan tingkat eksposur risiko korupsi, serta menilai kewajaran sumber kekayaannya. Setiap transaksi PEP akan ditinjau dengan sangat cermat. Hubungan bisnis dengan PEP harus mendapat persetujuan Direksi/AML Officer. Selain itu, seluruh transaksi yang melibatkan Nasabah PEP dicatat dalam register tersendiri agar dapat dipantau dan ditinjau secara khusus oleh AML Officer. Setiap transaksi yang berada di luar profil wajar PEP tersebut akan dianggap mencurigakan sampai terbukti sebaliknya.

**3. Simplified Due Diligence (SDD):**

*Nasabah Berisiko Lebih Rendah:* Dalam kondisi terbatas yang diizinkan regulasi (misal Nasabah merupakan lembaga keuangan berlisensi yang juga menerapkan APU/PPT, atau transaksi bernilai sangat kecil di bawah ambang tertentu), Perusahaan dapat menerapkan prosedur due diligence yang disederhanakan. Namun, saat ini Perusahaan cenderung tidak menggunakan SDD secara luas mengingat sektor kripto dianggap berisiko tinggi oleh regulator​file-b2ykmf7wrqem7zpyx9hqtm. Setiap penerapan SDD harus didasarkan pada hasil risk assessment yang menunjukkan risiko Nasabah benar-benar rendah dan bukan PEP. SDD dapat berupa pengumpulan data identitas yang terbatas dan pengecekan minimal, tetapi tidak mengabaikan kewajiban inti (identifikasi, verifikasi, dan screening sanksi tetap dilakukan)​file-b2ykmf7wrqem7zpyx9hqtm.

**4. Ongoing Due Diligence:** KYC tidak berhenti pada saat onboarding Nasabah, tetapi berlangsung terus-menerus. Perusahaan melakukan pemantauan dan pembaruan data Nasabah secara berkala​file-b2ykmf7wrqem7zpyx9hqtm:

*Pembaruan Data:* Secara periodik (misal setiap 1 tahun untuk risiko rendah, lebih sering untuk risiko tinggi), Perusahaan meminta Nasabah memperbarui informasi KYC mereka. Pembaruan mencakup validasi apakah dokumen identitas masih berlaku, apakah alamat atau pekerjaan berubah, dsb. Jika Nasabah tidak aktif dalam periode lama dan kembali bertransaksi, data KYC akan diverifikasi ulang sebelum melanjutkan transaksi​file-b2ykmf7wrqem7zpyx9hqtm.

*Monitoring Perubahan Status:* Jika diketahui informasi baru bahwa Nasabah menjadi PEP, terlibat kasus hukum, atau pindah ke negara berisiko, Perusahaan akan menyesuaikan klasifikasi risiko dan melakukan *due diligence* tambahan. AML Officer harus selalu siap menanggapi “trigger event” seperti berita negatif tentang Nasabah (misal terkait tindak pidana finansial) dengan meninjau ulang hubungan bisnis​file-b2ykmf7wrqem7zpyx9hqtm.

*Transaksi Tidak Sesuai Profil:* Bagian pemantauan transaksi (dijelaskan di seksi berikutnya) juga merupakan bagian dari ongoing CDD. Jika ditemukan transaksi yang tidak konsisten dengan profil Nasabah (contoh: volume jauh lebih besar dari biasanya, atau frekuensi meningkat drastis tanpa alasan jelas), maka Perusahaan akan melakukan tindakan KYC ulang/EDD pada Nasabah tersebut​file-b2ykmf7wrqem7zpyx9hqtm. Tindakan tersebut dapat berupa meminta klarifikasi dan dokumen tambahan sebelum melanjutkan hubungan bisnis.

*Pencatatan dan Bukti KYC:* Seluruh proses KYC/CDD/EDD didokumentasikan dengan baik. Formulir KYC, salinan dokumen identitas, hasil pencarian PEP/sanksi, korespondensi dengan Nasabah, catatan keputusan menerima atau menolak Nasabah, dan dokumen sumber dana semuanya disimpan dalam arsip Perusahaan (fisik maupun elektronik). Perusahaan memastikan dokumentasi ini dapat ditelusuri untuk membuktikan kepatuhan terhadap penerapan CDD​file-b2ykmf7wrqem7zpyx9hqtm. Data dan dokumen KYC akan disimpan minimal 5 tahun sejak berakhirnya hubungan dengan Nasabah atau sejak transaksi terakhir​file-b2ykmf7wrqem7zpyx9hqtm (lihat juga bagian Penyimpanan Data).

Dengan kebijakan KYC/CDD/EDD di atas, Perusahaan berupaya mengenali Nasabahnya secara memadai sehingga potensi penyalahgunaan jasa Perusahaan oleh pihak yang tidak bertanggung jawab dapat dicegah sedini mungkin​file-b2ykmf7wrqem7zpyx9hqtm.

**Pemantauan Transaksi**

Perusahaan melakukan monitoring transaksi secara berkesinambungan untuk mendeteksi aktivitas yang tidak wajar atau mencurigakan. Mengingat Perusahaan beroperasi sebagai merchant P2P di Binance, monitoring mencakup alur aset kripto pada platform serta alur dana fiat di rekening bank Perusahaan​file-b2ykmf7wrqem7zpyx9hqtm. Komponen-komponen pemantauan transaksi antara lain:

*Pemantauan Real-time di Platform Binance:* Platform Binance menyediakan dashboard transaksi yang memungkinkan merchant melihat order masuk, volume, dan data pengguna lawan transaksi. Petugas operasional Perusahaan memantau transaksi yang berlangsung secara real-time. Jika ada transaksi dalam jumlah sangat besar atau frekuensi tidak biasa dalam waktu singkat, petugas akan menandai dan memberitahu AML Officer untuk dianalisis lebih lanjut sebelum konfirmasi final​file-b2ykmf7wrqem7zpyx9hqtm. Misalnya, jika terdeteksi banyak transaksi pecah-belah (*smurfing*) dari satu pengguna atau kelompok pengguna ke Perusahaan di hari yang sama, hal itu akan diendus sebagai pola mencurigakan.

*Aturan dan Alarm (Red Flags):* Perusahaan menetapkan kriteria sinyal bahaya (*red flag*) yang akan memicu penelaahan lebih lanjut. Contoh *red flag*​file-b2ykmf7wrqem7zpyx9hqtm:

* Transaksi tunggal atau kumulatif dalam periode tertentu melebihi nilai tertentu (threshold internal) yang tidak lazim bagi Nasabah tersebut.
* Pola transaksi yang tidak sesuai profil (misal Nasabah yang biasanya membeli kripto senilai < Rp50 juta per minggu tiba-tiba melakukan transaksi Rp500 juta).
* Nasabah meminta metode pembayaran/penarikan yang kompleks atau melalui pihak ketiga.
* Indikasi strukturisasi – Nasabah terlihat sengaja membagi transaksi menjadi nominal kecil-kecil untuk menghindari perhatian.
* Adanya hubungan antara beberapa akun Binance yang bertransaksi dengan Perusahaan (misal beberapa akun berbeda tetapi rekening bank pengirim sama atau terafiliasi).
* Permintaan dari Nasabah untuk mengeksekusi transaksi dengan cara yang menyimpang dari prosedur normal platform (contoh: ingin bertransaksi di luar escrow Binance, permintaan yang tentu akan ditolak oleh Perusahaan)​file-b2ykmf7wrqem7zpyx9hqtm​file-b2ykmf7wrqem7zpyx9hqtm.

AML Officer menyusun daftar *red flag* berdasarkan panduan regulator dan pengalaman industri, serta memastikan sistem/pegawai dapat mengenalinya​file-b2ykmf7wrqem7zpyx9hqtm.

*Analisis Pasca-Transaksi:* Selain monitoring langsung, AML Officer secara rutin (misal mingguan) melakukan analisis agregat atas transaksi: merangkum volume total, frekuensi, pola per Nasabah. Laporan analisis ini membantu mengidentifikasi anomali yang luput dari pemantauan harian. Notula/rekap analisis transaksi disimpan sebagai catatan. Jika ditemukan anomali, akan dibandingkan dengan profil Nasabah terkait. Contoh, jika Nasabah A dalam sebulan terakhir melakukan puluhan kali transaksi dengan total jauh di atas perkiraan awal, AML Officer akan mengkaji apakah sumber dana Nasabah A wajar dan meminta klarifikasi ke Nasabah bila perlu​file-b2ykmf7wrqem7zpyx9hqtm.

*Sistem/Tools Monitoring:* Apabila volume transaksi meningkat, Perusahaan akan mempertimbangkan penggunaan perangkat lunak AML untuk memantau transaksi secara otomatis (misal software yang dapat memindai pola mencurigakan atau melakukan *flagging* otomatis). Namun, pada tahap awal operasional dengan volume terbatas, kombinasi monitoring manual harian dan review berkala oleh AML Officer dianggap memadai​file-b2ykmf7wrqem7zpyx9hqtm.

*Pemantauan Aliran Dana Fiat:* Setiap penerimaan atau pengiriman dana melalui rekening bank Perusahaan dicatat. Bagian keuangan melakukan rekonsiliasi untuk memastikan setiap dana masuk/keluar terkait transaksi P2P yang sah. Apabila ada dana masuk yang tidak diketahui asalnya atau tidak cocok dengan catatan transaksi, dana tersebut akan ditahan dan diselidiki. Begitu pula, Perusahaan memastikan rekening bank hanya digunakan untuk transaksi bisnis yang sah dan bukan untuk menampung dana pribadi di luar konteks perdagangan kripto, guna memudahkan pelacakan​file-b2ykmf7wrqem7zpyx9hqtm​file-b2ykmf7wrqem7zpyx9hqtm.

*Pemantauan Alamat Kripto (jika berlaku):* Apabila Perusahaan perlu mengirim atau menerima aset kripto dari/ke dompet pribadi di luar Binance (misalnya untuk mengisi saldo di Binance atau menarik keuntungan keluar), AML Officer akan memantau alamat dompet kripto yang terlibat. Sebelum mengirim ke dompet eksternal milik Nasabah, Perusahaan akan meminta konfirmasi kepemilikan dompet tersebut oleh Nasabah dan melakukan pengecekan dasar (misal melalui blockchain explorer atau alat analitik) apakah alamat tersebut terkait layanan mixer, darknet, atau aktivitas ilegal yang diketahui​file-b2ykmf7wrqem7zpyx9hqtm. Langkah ini untuk memenuhi prinsip Travel Rule apabila transfer on-chain dilakukan; data pengirim/penerima akan dicatat. Jika terdeteksi alamat bermasalah (tercantum dalam daftar hitam terkait kejahatan), Perusahaan dapat menolak atau menunda transaksi hingga *due diligence* tambahan dilakukan​file-b2ykmf7wrqem7zpyx9hqtm.

*Investigasi Internal:* Bila suatu transaksi atau pola transaksi memenuhi kriteria mencurigakan, AML Officer akan melakukan investigasi internal. Langkah-langkahnya meliputi: pengumpulan informasi transaksi terkait (jumlah, tanggal, pihak lawan, metode pembayaran), pemeriksaan kembali profil KYC Nasabah, penelusuran sumber dana (misal meninjau mutasi rekening Nasabah jika tersedia dalam dokumen yang diberikan), dan komunikasi dengan Nasabah untuk meminta penjelasan atas transaksi tersebut. Hasil investigasi ini dicatat dalam laporan hasil analisis internal​file-b2ykmf7wrqem7zpyx9hqtm.

*Tindakan Lanjutan:* Berdasarkan analisis, AML Officer memutuskan apakah:
a) Transaksi dapat dianggap wajar (*false alarm*) dan tidak perlu tindakan lanjut selain dicatat;
b) Transaksi mencurigakan dan perlu dilaporkan ke PPATK sebagai LTKM;
c) Hubungan dengan Nasabah perlu dihentikan (jika terindikasi kuat pelanggaran hukum atau ketidakpatuhan Nasabah);
d) Perlu dilakukan penyesuaian limit atau pengawasan khusus untuk Nasabah tersebut di masa mendatang​file-b2ykmf7wrqem7zpyx9hqtm.

Seluruh aktivitas monitoring di atas dirahasiakan dan Nasabah tidak diberi tahu jika transaksi mereka sedang ditelaah khusus, untuk mencegah *tipping off*. Pemantauan transaksi ini krusial untuk memastikan bahwa kegiatan bisnis Perusahaan tetap dalam koridor legal dan tidak disalahgunakan pihak yang mencoba mencuci uang atau mendanai terorisme​file-b2ykmf7wrqem7zpyx9hqtm.

**Pelaporan Transaksi Mencurigakan**

Perusahaan, sebagai entitas yang diwajibkan (Pihak Pelapor) berdasarkan UU 8/2010, wajib menyampaikan Laporan Transaksi Keuangan Mencurigakan (LTKM) kepada PPATK apabila ditemukan indikasi kuat adanya transaksi mencurigakan. Prosedur pelaporan ini meliputi​file-b2ykmf7wrqem7zpyx9hqtm:

*Identifikasi Insiden Mencurigakan:* Setelah AML Officer melakukan investigasi dan menyimpulkan bahwa suatu transaksi atau aktivitas Nasabah tergolong Transaksi Mencurigakan sesuai kriteria UU (lihat Definisi TKM), AML Officer akan menyiapkan laporan resmi. Indikasi umum transaksi mencurigakan misalnya: transaksi tidak sesuai profil dan tidak dapat dijelaskan secara masuk akal oleh Nasabah, upaya jelas menghindari pelaporan (misal memecah transaksi), penggunaan dana yang diduga ilegal, atau terdapat berita bahwa Nasabah terkait tindak pidana​file-b2ykmf7wrqem7zpyx9hqtm.

*Penyusunan Laporan:* AML Officer mengisi laporan TKM sesuai format yang ditentukan PPATK (Formulir LTKM). Laporan mencakup informasi seperti: identitas lengkap Nasabah, detail transaksi (tanggal, jumlah, jenis aset, rekening/domapet yang terlibat), uraian mengapa transaksi dicurigai (narasi pola dan alasan kecurigaan), serta dokumen pendukung (misal hasil analisis internal, korespondensi). Laporan ini ditandatangani/didisahkan oleh AML Officer atau Direksi yang bertanggung jawab​file-b2ykmf7wrqem7zpyx9hqtm.

*Batas Waktu Pelaporan:* Perusahaan akan mengirimkan LTKM sesegera mungkin, paling lambat 3 (tiga) hari kerja setelah diketahui adanya indikasi kuat transaksi mencurigakan​file-b2ykmf7wrqem7zpyx9hqtm. Batas waktu ini sesuai ketentuan yang berlaku di Indonesia. AML Officer memastikan tidak ada keterlambatan; proses investigasi internal pun diupayakan cepat agar memenuhi tenggat. Jika indikasi mencurigakan terkonfirmasi pada hari itu, idealnya laporan dikirim sebelum akhir hari ketiga berikutnya.

*Metode Penyampaian:* LTKM disampaikan kepada PPATK melalui sistem pelaporan elektronik yang ditentukan (misal *goAML*) atau sarana lain sesuai peraturan PPATK. AML Officer harus terdaftar sebagai Petugas Pelapor di PPATK. Bukti penerimaan laporan oleh PPATK (tanda terima elektronik) disimpan oleh Perusahaan​file-b2ykmf7wrqem7zpyx9hqtm.

*Kerahasiaan:* Laporan TKM bersifat rahasia. Dilarang keras bagi Perusahaan dan staf untuk memberitahukan kepada Nasabah atau pihak lain bahwa suatu transaksi telah atau akan dilaporkan ke PPATK​file-b2ykmf7wrqem7zpyx9hqtm. Informasi terkait pelaporan hanya boleh diketahui oleh pihak internal yang berwenang (AML Officer, Direksi) dan otoritas terkait. Pelanggaran kerahasiaan ini (*tipping off*) dapat berakibat sanksi pidana sesuai UU 8/2010.

*Pelaporan Transaksi Tunai dan Transfer Dana:* Meskipun bisnis Perusahaan umumnya tidak berurusan dengan uang tunai secara fisik, jika dalam operasional terdapat Transaksi Keuangan Tunai di atas ambang batas yang ditetapkan regulator (misalnya ≥ Rp500 juta dalam satu hari, sesuai ketentuan PPATK untuk Laporan Transaksi Keuangan Tunai/LTKT), Perusahaan juga akan melaporkannya. Demikian pula, jika ada transaksi transfer dana lintas negara di luar platform Binance (contoh: Perusahaan menerima kiriman uang dari luar negeri untuk pembelian kripto), dan memenuhi kriteria Laporan Transaksi Transfer Dana (LTKL), maka akan dilaporkan sesuai aturan​file-b2ykmf7wrqem7zpyx9hqtm. Namun, kondisi ini diusahakan tidak terjadi atau minimal, mengingat Perusahaan membatasi transaksi pada domestik IDR melalui bank lokal.

*Koordinasi dengan Binance:* Jika transaksi mencurigakan melibatkan akun di platform Binance, Perusahaan akan berkoordinasi seperlunya dengan tim keamanan/AML Binance (sesuai panduan Binance). Misalnya, jika Perusahaan melaporkan Nasabah X ke PPATK, Binance juga perlu diberi tahu agar mereka dapat mengambil tindakan di level platform (pembekuan akun secara preventif). Koordinasi ini dilakukan setelah laporan ke PPATK dikirim, dan terbatas pada pertukaran informasi yang diizinkan, dengan tetap menjaga kerahasiaan dari subjek (Nasabah)​file-b2ykmf7wrqem7zpyx9hqtm.

*Penerimaan Permintaan Informasi:* Apabila PPATK atau penyidik meminta informasi atau dokumen tambahan terkait laporan yang disampaikan, Perusahaan akan merespons dengan cepat dan lengkap. AML Officer bertanggung jawab sebagai kontak yang akan memberikan data pendukung investigasi, sesuai kewenangan yang diatur UU​file-b2ykmf7wrqem7zpyx9hqtm.

Dengan mekanisme di atas, Perusahaan memastikan kewajiban pelaporan dipenuhi. Perusahaan menyadari bahwa LTKM adalah fondasi utama program APU untuk mendeteksi dan menghentikan kejahatan keuangan lebih awal​file-b2ykmf7wrqem7zpyx9hqtm. Kegagalan melapor bukan saja berisiko sanksi hukum bagi Perusahaan​file-b2ykmf7wrqem7zpyx9hqtm, tapi juga dapat merusak reputasi dan integritas perusahaan. Oleh karena itu, setiap indikasi transaksi mencurigakan akan ditindaklanjuti dengan serius.

**Penyimpanan Data dan Perlindungan Informasi**

Perusahaan berkomitmen menjaga penyimpanan data terkait APU/PPT dengan aman dan sesuai jangka waktu yang diwajibkan. Selain itu, perlindungan kerahasiaan data Nasabah juga menjadi prioritas, sejalan dengan prinsip perlindungan data pribadi. Kebijakan terkait hal ini antara lain:

*Retensi Data 5 Tahun:* Seluruh dokumen dan informasi yang diperoleh dalam rangka penerapan KYC/CDD (misalnya formulir nasabah, fotokopi identitas, bukti alamat, hasil pengecekan, komunikasi terkait) serta catatan transaksi dan hasil analisis transaksi, wajib disimpan sekurang-kurangnya selama 5 (lima) tahun sejak hubungan usaha berakhir dengan Nasabah atau sejak transaksi dilakukan (mana yang lebih lama)​file-b2ykmf7wrqem7zpyx9hqtm. Ketentuan ini sesuai standar internasional dan regulasi OJK/Bappebti. Perusahaan dapat menetapkan masa simpan lebih panjang jika diperlukan oleh aturan lain atau jika masih dibutuhkan dalam investigasi yang sedang berjalan.

*Media Penyimpanan:* Data disimpan dalam bentuk hardcopy (dokumen fisik) dan softcopy (digital). Untuk dokumen fisik, Perusahaan menyimpan arsip dalam lemari arsip terkunci di kantor yang hanya dapat diakses oleh personel berwenang (AML Officer atau staf yang ditunjuk). Untuk data digital, disimpan di sistem komputer/sistem *cloud* perusahaan dengan akses terbatas (dilindungi password) dan backup rutin. Perusahaan melakukan backup data penting secara berkala agar tidak hilang jika terjadi kerusakan sistem​file-b2ykmf7wrqem7zpyx9hqtm.

*Keamanan Informasi:* Perusahaan menerapkan langkah-langkah keamanan informasi untuk melindungi data Nasabah dari akses tidak sah atau kebocoran. Termasuk di dalamnya: penggunaan enkripsi untuk data elektronik sensitif, kontrol akses berjenjang (hanya AML Officer dan Direktur yang dapat mengakses semua data APU/PPT, staf lain hanya sesuai kebutuhan tugas), firewall dan anti-malware pada perangkat komputer, serta kebijakan *clear desk* (tidak meninggalkan dokumen sensitif tergeletak terbuka). Jika data disimpan di layanan cloud, dipastikan penyedia cloud memiliki standar keamanan tinggi dan servernya (jika mungkin) berlokasi dengan perlindungan hukum memadai​file-b2ykmf7wrqem7zpyx9hqtm​file-b2ykmf7wrqem7zpyx9hqtm.

*Kerahasiaan dan NDA:* Seluruh pegawai yang menangani data Nasabah diharuskan menandatangani Perjanjian Kerahasiaan (NDA) internal. Pelanggaran atas kerahasiaan data Nasabah atau data pelaporan APU/PPT akan dikenakan sanksi tegas, termasuk pemecatan dan pelaporan pidana jika ada unsur kesengajaan membocorkan​file-b2ykmf7wrqem7zpyx9hqtm.

*Penggunaan Data Pribadi:* Informasi pribadi Nasabah yang dikumpulkan Perusahaan hanya digunakan untuk keperluan APU/PPT dan kepatuhan hukum, serta untuk keperluan operasional transaksi terkait. Perusahaan tunduk pada prinsip minimasi data – hanya mengumpulkan data yang relevan – dan melindungi hak privasi Nasabah sesuai ketentuan perundangan (termasuk UU Perlindungan Data Pribadi, jika berlaku). Penyampaian data Nasabah ke pihak ketiga hanya dilakukan atas dasar ketentuan hukum (misal permintaan PPATK, penyidik, regulator) atau persetujuan Nasabah​file-b2ykmf7wrqem7zpyx9hqtm.

*Penghancuran Data:* Setelah masa retensi 5 tahun berlalu dan data tidak lagi diperlukan (serta tidak ada perintah retensi lebih lama dari regulator), Perusahaan akan memusnahkan data tersebut secara aman. Dokumen fisik dihancurkan (shredding) sedemikian rupa agar tidak dapat dibaca ulang, sedangkan file digital dihapus permanen (*secure erase*) dari penyimpanan​file-b2ykmf7wrqem7zpyx9hqtm.

Dengan langkah-langkah di atas, Perusahaan memastikan dua hal: (1) Data historis tersedia untuk mendukung investigasi atau audit di masa mendatang (misal, saat diminta regulator, Perusahaan dapat menunjukkan rekam jejak KYC dan transaksi Nasabah tertentu hingga 5 tahun ke belakang)​file-b2ykmf7wrqem7zpyx9hqtm; (2) Data tersebut tidak disalahgunakan atau diakses pihak yang tidak berwenang, sehingga privasi Nasabah tetap terlindungi. Kepatuhan terhadap penyimpanan dan perlindungan data ini bukan hanya kewajiban regulasi, tetapi juga bagian dari komitmen Perusahaan untuk menjaga kepercayaan Nasabah dan integritas operasional.

**Pelatihan dan Audit Internal**

*Pelatihan (Training) APU/PPT:* Perusahaan akan menyelenggarakan program pelatihan berkala bagi seluruh personel terkait (terutama yang terlibat dalam proses penerimaan Nasabah, operasional transaksi, dan manajemen). Pelatihan mencakup: pemahaman dasar TPPU dan pendanaan terorisme, kewajiban hukum APU/PPT, cara melakukan KYC yang benar, mengenali tanda-tanda transaksi mencurigakan, prosedur pelaporan internal, sanksi atas ketidakpatuhan, serta update terbaru (misal modus pencucian uang terkini atau pembaruan regulasi)​file-b2ykmf7wrqem7zpyx9hqtm.

*Frekuensi Pelatihan:* Minimal satu kali dalam setahun untuk seluruh staf, dan pelatihan awal (on-boarding) segera diberikan bagi karyawan baru sebelum menangani tugas terkait AML. Untuk staf kunci seperti AML Officer atau tim compliance, diupayakan mengikuti workshop eksternal atau sertifikasi (misal sertifikasi AML) sesuai kebutuhan agar kompetensi terjaga​file-b2ykmf7wrqem7zpyx9hqtm.

*Metode:* Pelatihan dapat berupa kelas in-house, webinar, modul e-learning, maupun simulasi kasus. Contohnya, Perusahaan bisa mengadakan sesi *case study* di mana pegawai diminta mengidentifikasi apakah suatu skenario transaksi fiktif mencurigakan atau tidak, guna menguji pemahaman​file-b2ykmf7wrqem7zpyx9hqtm.

*Dokumentasi Pelatihan:* Kehadiran dan materi pelatihan didokumentasikan (notula, slide presentasi, daftar hadir) sebagai bukti kepada regulator bahwa program pelatihan dijalankan​file-b2ykmf7wrqem7zpyx9hqtm.

*Audit Internal Berkala:* Setidaknya sekali setahun, Direksi menugaskan fungsi audit internal (atau pihak independen eksternal jika perusahaan belum memiliki unit audit) untuk melakukan review menyeluruh atas program APU/PPT. Audit mencakup pemeriksaan sampel dokumen KYC, pengujian apakah penilaian risiko dilaksanakan dan didokumentasikan, verifikasi bahwa transaksi telah dimonitor dan laporan mencurigakan (jika ada) dikirim tepat waktu, serta kepatuhan terhadap penyimpanan data. Hasil audit ini dituangkan dalam laporan tertulis yang memuat temuan dan rekomendasi perbaikan. Laporan audit disampaikan ke Direksi dan ditindaklanjuti oleh AML Officer​file-b2ykmf7wrqem7zpyx9hqtm.

*Uji Kepatuhan (Compliance Testing):* Secara rutin, AML Officer dapat melakukan uji acak (spot check) internal. Misal: memeriksa 5 nasabah terakhir apakah dokumen KYC lengkap, atau memeriksa log transaksi minggu lalu apakah ada *red flag* yang terlewat. Ini membantu deteksi dini kekurangan operasional​file-b2ykmf7wrqem7zpyx9hqtm.

*Tinjauan Manajemen:* Direksi bersama AML Officer setiap kuartal (3 bulan) melakukan rapat evaluasi singkat terkait APU/PPT: membahas tren transaksi, kendala penerapan, update regulasi, dan apakah sumber daya cukup. Notulen rapat tersebut disimpan​file-b2ykmf7wrqem7zpyx9hqtm.

*Perbaikan Berkelanjutan:* Apabila ada temuan audit atau insiden (misal ternyata ada transaksi mencurigakan terlewat lapor), Perusahaan segera melakukan tindakan korektif: revisi prosedur, pelatihan tambahan, atau penambahan tenaga. Perusahaan berkomitmen melakukan improvement berkelanjutan agar program APU/PPT selalu efektif dan up to date​file-b2ykmf7wrqem7zpyx9hqtm.

Dengan pelatihan yang memadai dan audit internal yang ketat, diharapkan seluruh mekanisme APU/PPT Perusahaan tidak hanya ada di dokumen, tetapi benar-benar dijalankan dan diawasi. Hal ini juga membantu Perusahaan dalam menghadapi audit eksternal dari regulator ataupun penilaian Binance atas kepatuhan merchant (misal melalui kuesioner AML, visitasi, dsb.), karena dapat menunjukkan bukti implementasi nyata​file-b2ykmf7wrqem7zpyx9hqtm.

**Kanal Pelaporan Pelanggaran (Whistleblowing)**

Perusahaan menyediakan mekanisme pelaporan pelanggaran secara anonim (*whistleblowing*) untuk mendorong pengungkapan dini setiap tindakan atau situasi yang melanggar kebijakan APU/PPT. Kanal ini memungkinkan karyawan atau pihak lain yang melihat adanya penyimpangan melapor tanpa rasa takut akan pembalasan. Ketentuan kanal pelaporan ini meliputi:

*Saluran Pelaporan:* Perusahaan menetapkan saluran khusus yang dapat diakses 24/7, misalnya: alamat email anonim (contoh: **compliance@digitalvault.co.id**) yang langsung diteruskan ke Komisaris Independen atau Direktur yang tidak terlibat sehari-hari; kotak pengaduan fisik di kantor yang hanya dibuka oleh pejabat tertentu; atau formulir online anonim. Informasi tentang kanal ini disosialisasikan kepada seluruh pegawai (misal dalam buku pedoman atau papan pengumuman internal). *(Catatan: detail kontak kanal tersedia dalam Lampiran Prosedur Whistleblowing).*​file-b2ykmf7wrqem7zpyx9hqtm

*Perlindungan Whistleblower:* Perusahaan menjamin kerahasiaan identitas pelapor. Laporan bisa dilakukan tanpa menyebut nama. Jika pelapor mencantumkan identitas, identitas tersebut hanya diketahui oleh pihak penerima laporan dan tidak akan disebarluaskan tanpa persetujuan pelapor. Perusahaan melarang segala bentuk retaliasi (pembalasan negatif) terhadap pelapor yang beritikad baik. Setiap pelapor yang mengalami intimidasi atau diskriminasi akibat melapor akan mendapatkan perlindungan dan pelaku pembalasan dapat dikenakan sanksi​file-b2ykmf7wrqem7zpyx9hqtm.

*Tindak Lanjut:* Laporan yang masuk akan direview oleh tim independen (misal Komisaris Independen atau komite audit) untuk menentukan langkah investigasi selanjutnya. Jika laporan terbukti, Perusahaan akan mengambil tindakan sesuai ketentuan (misal sanksi disipliner bagi pelaku pelanggaran, perbaikan prosedur). Contoh, jika terungkap seorang pegawai memalsukan dokumen KYC demi meluluskan Nasabah, pegawai tersebut akan diberi sanksi dan seluruh KYC Nasabah terkait akan ditinjau ulang. Apabila laporan ternyata tidak terbukti (misal kesalahpahaman), kasus ditutup dengan tetap melindungi pelapor​file-b2ykmf7wrqem7zpyx9hqtm.

*Pencatatan:* Semua laporan whistleblowing dicatat dalam Register Pengaduan dengan kode unik (tanpa mencantumkan nama pelapor bila anonim). Isi laporan, hasil investigasi, dan keputusan akhir didokumentasikan. Data ini dilaporkan ringkasannya kepada Direksi/Komisaris secara periodik untuk memastikan mekanisme ini berjalan​file-b2ykmf7wrqem7zpyx9hqtm.

Penerapan kanal pelaporan pelanggaran ini penting untuk menciptakan lingkungan di mana pegawai merasa bertanggung jawab dan berani *speak-up* jika melihat hal janggal. Hal ini menambah lapisan perlindungan bagi Perusahaan terhadap kemungkinan adanya kelalaian atau kecurangan internal yang dapat melemahkan program APU/PPT​file-b2ykmf7wrqem7zpyx9hqtm.

**Penunjukan Pejabat Penanggung Jawab AML**

Sesuai peraturan, Perusahaan menunjuk seorang Pejabat Penanggung Jawab APU/PPT (AML Compliance Officer). Rincian penunjukan dan peran pejabat ini adalah sebagai berikut:

*Identitas Pejabat:* Perusahaan telah menunjuk **[Nama Pejabat yang Ditunjuk]** sebagai AML Compliance Officer. *(Saat dokumen ini disahkan, jabatan tersebut dipegang oleh Direktur Utama Perusahaan, Aleksei Baum, untuk sementara hingga ditunjuk personel khusus.)* Penunjukan ini ditetapkan melalui Surat Keputusan Direksi dan dilaporkan kepada otoritas (jika disyaratkan oleh BAPPEBTI/OJK)​file-b2ykmf7wrqem7zpyx9hqtm.

*Kualifikasi:* Pejabat ini memiliki pengetahuan yang memadai tentang regulasi APU/PPT dan operasi bisnis perusahaan. Telah atau sedang mengikuti pelatihan khusus AML. Kompetensi dan rekam jejaknya memenuhi ekspektasi regulator maupun Binance (sebagai mitra platform)​file-b2ykmf7wrqem7zpyx9hqtm.

*Wewenang:* AML Officer memiliki akses penuh ke informasi yang diperlukan (data Nasabah, data transaksi) dan wewenang untuk mengambil keputusan independen terkait pencegahan pencucian uang. Ia dapat berkomunikasi langsung dengan Direksi atau Komisaris tanpa hambatan. Pejabat ini juga berwenang menghentikan sementara suatu transaksi atau menolak menjalankan instruksi bisnis jika menurut analisanya berisiko melanggar ketentuan APU/PPT, sambil melapor segera ke Direksi​file-b2ykmf7wrqem7zpyx9hqtm.

*Tugas Utama:* Secara ringkas, AML Officer:

* Mengawasi pelaksanaan seluruh komponen kebijakan ini (KYC, monitoring, pelaporan).
* Memberikan arahan harian kepada staf operasional terkait penerapan KYC dan deteksi transaksi mencurigakan.
* Menjadi penghubung dengan PPATK, OJK/Bappebti, dan penegak hukum dalam hal apapun terkait kewajiban APU/PPT, termasuk menerima surat edaran atau permintaan informasi.
* Menyusun dan mengirim laporan-laporan wajib (LTKM, laporan berkala APU/PPT ke regulator jika ada).
* Meng-update kebijakan internal apabila ada perubahan regulasi atau kebijakan Binance yang relevan.
* Melaporkan secara berkala kepada Direksi tentang efektivitas program APU/PPT, termasuk jumlah nasabah high-risk, jumlah laporan mencurigakan yang dikirim, kendala yang dihadapi, dll.​file-b2ykmf7wrqem7zpyx9hqtm​file-b2ykmf7wrqem7zpyx9hqtm

*Independensi:* AML Officer tidak boleh merangkap tugas yang menimbulkan benturan kepentingan (misal tidak terlibat langsung dalam penjualan/pemasaran yang targetnya bisa membuat abai terhadap risiko). Jika AML Officer adalah Direktur sendiri, maka Direksi berkomitmen menjalankan fungsi tersebut dengan objektif dan siap diaudit​file-b2ykmf7wrqem7zpyx9hqtm​file-b2ykmf7wrqem7zpyx9hqtm.

*Penggantian/Penonaktifan:* Jika AML Officer berhalangan tetap atau mengundurkan diri, Perusahaan secepatnya menunjuk pengganti dan selama masa transisi Direksi mengambil alih tugas tersebut. Hal ini untuk memastikan tidak ada kekosongan fungsi kepatuhan​file-b2ykmf7wrqem7zpyx9hqtm.

Penunjukan AML Compliance Officer merupakan manifestasi tanggung jawab Perusahaan pada level manajemen puncak untuk memastikan program APU/PPT berjalan. Nama dan kontak AML Officer dicantumkan dalam dokumen ini dan dapat diberikan kepada pihak berwenang atau mitra bisnis bila diperlukan.

**Lampiran**

* **Daftar Yurisdiksi Berisiko Tinggi** – berisi daftar negara-negara (atau yurisdiksi) yang dikategorikan berisiko tinggi atau berada dalam status pengawasan intensif berdasarkan penilaian FATF dan Uni Eropa. Contohnya: Korea Utara, Iran, Myanmar, Afghanistan, Nigeria, Afrika Selatan, Suriah, Yaman, dan lain-lain. Daftar ini digunakan sebagai acuan dalam penilaian risiko geografis Nasabah dan diperbarui secara berkala sesuai publikasi resmi terbaru.
* **Formulir KYC Nasabah (Individual)** – berisi isian data pribadi Nasabah perorangan: nama, alamat, tanggal lahir, kewarganegaraan, nomor identitas (KTP/Paspor), NPWP (jika ada), pekerjaan, sumber penghasilan, tujuan bertransaksi, serta pernyataan kebenaran informasi. Nasabah wajib mengisi dan menandatangani formulir ini saat onboarding (bila di luar platform Binance). Formulir ini mencakup bagian untuk data Beneficial Owner (jika Nasabah bertindak untuk pihak lain) dan pernyataan kesediaan mematuhi ketentuan APU/PPT Perusahaan​file-b2ykmf7wrqem7zpyx9hqtm.
* **Formulir Deklarasi PEP** – formulir yang harus diisi Nasabah untuk menyatakan apakah ia atau kerabatnya merupakan Politically Exposed Person. Jika *Ya*, diuraikan jabatan publik yang dipegang, instansi, dan periode menjabat. Formulir ini juga mencakup pernyataan Nasabah bahwa dana yang digunakan bukan hasil korupsi/penyalahgunaan jabatan. Formulir ini membantu Perusahaan mendokumentasikan identifikasi PEP secara tertulis​file-b2ykmf7wrqem7zpyx9hqtm.
* **Formulir Pernyataan Sumber Dana** – digunakan untuk Nasabah dengan transaksi bernilai besar atau profil risiko tinggi. Nasabah menjelaskan asal usul dana yang akan dipakai dalam transaksi (misal: tabungan dari gaji, penjualan properti, warisan, investasi lain, dll.) dan menyatakan legalitas sumber tersebut. Dilengkapi tanda tangan Nasabah. Formulir ini penting sebagai bagian EDD untuk memastikan dana tidak berasal dari kejahatan​file-b2ykmf7wrqem7zpyx9hqtm.
* **Prosedur Whistleblowing & Formulir Pelaporan** – penjelasan tertulis singkat mengenai mekanisme pelaporan pelanggaran di Perusahaan, termasuk nomor/email pengaduan anonim. Disertai form standar (opsional diisi) bagi pelapor internal untuk menyampaikan laporannya (berisi kolom: deskripsi kejadian, waktu, pihak terlibat, bukti jika ada). Pelapor boleh mengosongkan identitas demi anonimitas. Prosedur ini disebarkan kepada seluruh karyawan (misal dalam buku pedoman atau papan pengumuman internal) agar diketahui​file-b2ykmf7wrqem7zpyx9hqtm.
* **Formulir Profil Nasabah & Penilaian Risiko** – lembar internal yang diisi oleh AML Officer saat proses KYC selesai. Berisi rangkuman informasi kunci Nasabah (nama, usia, pekerjaan, PEP/Non-PEP, negara domisili, sumber dana, dsb.), kategori risiko yang ditetapkan (Low/Medium/High) beserta alasan/justifikasi singkat, dan keputusan apakah menerima Nasabah tersebut. Form ini ditandatangani AML Officer dan disetujui atasan (jika diperlukan untuk high-risk). Jika di kemudian hari ada perubahan profil atau *review*, form ini diperbarui atau dilampiri catatan perubahan​file-b2ykmf7wrqem7zpyx9hqtm.
* **Contoh Laporan LTKM (Suspicious Activity Report)** – template laporan Transaksi Mencurigakan yang akan dikirim ke PPATK. Meliputi contoh pengisian agar konsisten: data subjek, kronologi singkat transaksi mencurigakan, dan tabel transaksi. Template ini menjadi acuan internal agar setiap laporan yang disusun mengikuti format baku (Catatan: laporan aktual disampaikan via sistem PPATK)​file-b2ykmf7wrqem7zpyx9hqtm.
* **Pernyataan Komitmen Pegawai** – dokumen yang ditandatangani seluruh pegawai Perusahaan, berisi pernyataan bahwa mereka telah membaca dan memahami Kebijakan APU/PPT ini, serta berjanji untuk melaksanakannya dengan sungguh-sungguh. Pernyataan ini juga mencakup kesediaan menjaga kerahasiaan informasi Nasabah dan laporan (anti tipping-off), serta konsekuensi sanksi jika melanggar. Form ini biasanya ditandatangani saat sosialisasi kebijakan atau pelatihan pertama, dan disimpan di arsip SDM​file-b2ykmf7wrqem7zpyx9hqtm.

Semua lampiran di atas merupakan bagian tak terpisahkan dari Kebijakan APU/PPT Perusahaan. Lampiran-lampiran tersebut akan diperbarui sesuai kebutuhan (misal jika ada perubahan regulasi yang memerlukan penyesuaian form). Versi terbaru lampiran disimpan oleh AML Officer dan tersedia untuk diperlihatkan kepada auditor atau regulator​file-b2ykmf7wrqem7zpyx9hqtm.

**Persetujuan dan Pengesahan**

Dokumen “Kebijakan dan Prosedur APU/PPT” ini telah ditinjau dan disetujui oleh Direksi Perusahaan. Kebijakan mulai berlaku pada tanggal ditandatangani di bawah ini dan berlaku hingga ada pembaruan resmi. Seluruh jajaran PT Digital Asset Vault wajib mematuhi ketentuan dalam kebijakan ini​file-b2ykmf7wrqem7zpyx9hqtm.

*Denpasar, [Tanggal efektif kebijakan]*

PT Digital Asset Vault
Direktur Utama
Aleksei Baum