| **내부통제 지침** |
| --- |

**목 차**

[**1. 목적 4**](#_wr33wscx7ovo)

[**2. 적용 범위 4**](#_gvzmpekkftpp)

[**3. 내부통제 기본 원칙 4**](#_jsr09l9ao8n8)

[3.1 핫월렛과 콜드월렛 분리 운영 4](#_ob20x1ufl3gz)

[3.2 다중 서명(Multi-sig) 체계 운영 4](#_jhmsjiq1i4me)

[3.3 KYC/AML 준수 4](#_9zr77z90uu0w)

[3.4 시스템 접근 통제 4](#_ijh4siwsbrqk)

[3.5 투명한 거래 기록 유지 4](#_erbs6jawooh5)

[**4. 주요 내부통제 절차 4**](#_1aqhmlq2dtek)

[4.1 자산 관리 통제 5](#_6yuuwq60c7y5)

[4.2 이상 거래 탐지 시스템 (FDS) 5](#_bnd6dldd9cy6)

[4.3 개발 및 배포 통제 5](#_l8e7mpcm3gbk)

[4.4 내부 정보 보호 5](#_y85yvjfi5r7j)

[**5. 내부통제 책임자 및 보고체계 5**](#_tx9q92xvot6f)

[**6. 교육 및 인식 제고 5**](#_3aozf2lckdsp)

[**7. 내부 금융사고 발생 시 자금세탁방지 관점에서의 분석 및 대응 6**](#_b2d83iulnslc)

[7.1 발생 원인 분석 6](#_nai7r1a53kdk)

[7.2 대응 절차 6](#_7nza1v3yfh78)

[1. 즉각적 자산 이동 차단 조치 6](#_lubo82g2kg1x)

[2. 사고 보고 및 내부 공유 6](#_q1yq0ojngoq7)

[3. 의심거래 보고(SAR) 제출 6](#_oh4zei2n7sex)

[4. 내부 감사 착수 및 원인 규명 6](#_z3zydbp0pw92)

[5. 외부 전문기관 협조 7](#_7s3x867ypi74)

[6. 재발방지 대책 수립 7](#_77dsvslprc2s)

[7.3 재발 방지를 위한 제도화 방안 7](#_1iy229pi7g7)

[1. 내부자 행동 모니터링 시스템 구축 7](#_5qewwjecdzfj)

[2. 핫월렛 이체 한도 자동 조정 기능 도입 7](#_ms659wlydfiq)

[3. 거래 패턴 기반 AI 이상거래 탐지 시스템 고도화 7](#_c3n5efn4xppx)

[4. 내부자 대상 AML 윤리 교육 정기화 (연 2회 이상) 7](#_tfrms6sdl9sr)

[**8. 외부 금융사고 발생 시 자금세탁방지 관점에서의 분석 및 대응 7**](#_9hek8evh3sb0)

[8.1 발생 원인 분석 7](#_f02374impy68)

[8.2 대응 절차 8](#_4t17arjn7308)

[1. 이상 거래 실시간 감지 및 자동 보류 8](#_ggum8d8bbooz)

[2. 고객 계정 정지 및 확인 요청 8](#_urley2kt6erc)

[3. 의심거래 보고(SAR) 제출 8](#_ulwe7huah4uw)

[4. 외부 기관 및 제휴사 공조 8](#_2zd5k92g8lue)

[5. 피해 고객 보호 절차 진행 8](#_eirr4mjunp32)

[8.3 재발 방지를 위한 제도화 방안 8](#_87tj1mmue89k)

[1. 이상거래탐지 시스템(FDS) 고도화 8](#_5p1hq7o2963e)

[2. 피싱 방지 위한 고객 대상 보안 교육 강화 8](#_k8ugfivqbf3k)

[3. 고위험 국가 및 주소 리스크 평가 강화 8](#_ar81hjtmlby)

[**9. 위반 시 조치 9**](#_q29ma0ugta9t)

[**10. 지침의 검토 및 개정 9**](#_cbiqoh2379lo)

### **1. 목적**

본 지침은 가상자산과 관련된 업무를 수행하는 회사가 자산을 안전하게 보호하고, 고객 신뢰를 확보하며, 법적·윤리적 기준을 준수하도록 내부통제 체계를 수립하고 운영하는 것을 목적으로 한다.

### **2. 적용 범위**

이 지침은 회사의 전 임직원(정규직, 계약직, 외주 포함) 및 가상자산 거래, 보관, 개발 등과 관련된 모든 업무에 적용된다.

### **3. 내부통제 기본 원칙**

#### 3.1 핫월렛과 콜드월렛 분리 운영

* 고객 자산과 회사 자산은 철저히 분리하며, 고객 자산의 대부분은 콜드월렛에 보관한다.
* 핫월렛의 출금 한도는 일일 최대 출금량 기준으로 제한된다.

#### 3.2 다중 서명(Multi-sig) 체계 운영

* 중요 자산의 이동은 다중 서명 또는 관리자 2인 이상의 승인 절차를 거쳐야 한다.

#### 3.3 KYC/AML 준수

* 고객확인제도(KYC)를 도입하여, 가상자산이 익명성을 악용하지 않도록 한다.
* 자금세탁방지(AML) 시스템을 통해 고위험 거래 및 의심거래를 탐지한다.

#### 3.4 시스템 접근 통제

* 관리 콘솔 및 지갑 시스템은 VPN과 MFA(다단계 인증)를 필수로 사용.
* 권한은 최소한의 원칙(Least Privilege Principle)을 적용.

#### 3.5 투명한 거래 기록 유지

* 블록체인 상의 거래뿐 아니라 내부 관리시스템상의 로그도 별도로 저장 및 감사한다.

### **4. 주요 내부통제 절차**

#### 4.1 자산 관리 통제

* 입출금 트랜잭션은 실시간으로 로그 기록되며, 이상 징후 발생 시 자동 알림.
* 긴급상황(예: 해킹 시도) 발생 시 핫월렛 전면 차단 기능 운영.
* 월 1회 이상 콜드월렛 잔고 실사 및 검증 보고서 작성.

#### 4.2 이상 거래 탐지 시스템 (FDS)

* 다음 유형의 이상 거래 자동 탐지:
  + 고빈도 반복 거래
  + 신규 가입자의 고액 전송
  + 믹싱 서비스나 프라이버시 코인으로의 전송
* 탐지 시 자동 보류 및 내부 조사 착수.

#### 4.3 개발 및 배포 통제

* 코드 변경 시 Git 기반 버전관리 필수.
* 신규 기능은 반드시 테스트넷에서 시뮬레이션 후 운영 환경에 반영.
* 스마트 계약 배포 시 외부 보안 감사 필수.

#### 4.4 내부 정보 보호

* 미공개 정보에 대한 임직원의 사적 사용 금지 (예: 상장 정보).
* 내부자 거래 및 프론트러닝 행위 금지 및 감시 체계 구축.

### **5. 내부통제 책임자 및 보고체계**

| **구분** | **역할 및 책임** |
| --- | --- |
| **내부통제책임자 (CCO)** | 정책 수립, 위반 사례 조사 및 보고 |
| **정보보안책임자 (CISO)** | 시스템 접근통제, 보안 로그 감사 |
| **AML 담당자** | 의심거래 보고, 고객정보 검토 |
| **독립적 감사** | 분기별 통제 체계 감사 및 리포트 작성 |

### **6. 교육 및 인식 제고**

* 연 1회 이상 **가상자산 보안 교육, KYC/AML 교육** 실시.
* 신규 입사자 대상 필수 교육 이수 후 시스템 접근 권한 부여.

### **7. 내부 금융사고 발생 시 자금세탁방지 관점에서의 분석 및 대응**

#### 7.1 발생 원인 분석

| **분류** | **주요 원인** | **설명** |
| --- | --- | --- |
| **인적 요인** | 내부자 부정행위 | 자금세탁 조직과 연계된 내부자의 고의적 자산 유출, 위조 |
| **통제 부재** | 권한 관리 미흡 | 지갑 접근 권한이 과다하거나 이중 승인 없이 자산 이체 가능 |
| **시스템 문제** | 모니터링 미비 | 비정상 거래를 실시간으로 탐지하지 못함 |
| **KYC/거래 감시 미흡** | 허위 계정 통한 자금 이탈 | 타인 명의 계정 사용, 자산 분산 출금 등 비정상 패턴 탐지 실패 |
| **정보보안 취약** | 내부 시스템 침투 | 내부 통신망 또는 인증 시스템의 취약점을 이용한 자산 탈취 |

#### 7.2 대응 절차

##### 즉각적 자산 이동 차단 조치

* + 관련 지갑(핫월렛 등)의 출금 기능 일시 정지
  + 연관 계정의 입출금 제한 및 계정 동결

##### 사고 보고 및 내부 공유

* + 1시간 이내 **내부통제책임자(CCO), CISO, AML 책임자**에 즉시 보고
  + 사고 내용 및 조치 사항을 사고관리시스템에 등록

##### 의심거래 보고(SAR) 제출

* + 금융정보분석원(FIU) 또는 감독기관에 **의심거래보고서(SAR)** 작성 및 제출
  + 사고 관련 거래 내역, 계정 정보, 탐지 시점 등을 포함

##### 내부 감사 착수 및 원인 규명

* + 관련 로그, 승인 이력, 내부 이메일, 접근기록 등 조사
  + 관련자 면담 및 책임 규명 절차 수행

##### 외부 전문기관 협조

* + 필요 시 **블록체인 분석 전문기관**, 법무팀, 보안 전문가 등과 협력하여 자산 추적

##### 재발방지 대책 수립

* + 사고 원인 기반 내부통제 시스템 개선안 도출
  + 정책/시스템/교육 등 전방위 재점검 및 보완

#### 7.3 재발 방지를 위한 제도화 방안

##### 내부자 행동 모니터링 시스템 구축

예: 이상 로그인, 업무 외 시간대 지갑 접근 감시

##### 핫월렛 이체 한도 자동 조정 기능 도입

예: 급증한 출금 요청 발생 시 자동 보류 및 관리자 승인 의무화

##### 거래 패턴 기반 AI 이상거래 탐지 시스템 고도화

##### 내부자 대상 AML 윤리 교육 정기화 (연 2회 이상)

### **8. 외부 금융사고 발생 시 자금세탁방지 관점에서의 분석 및 대응**

#### 8.1 발생 원인 분석

| **분류** | **주요 원인** | **설명** |
| --- | --- | --- |
| **이용자 계정 탈취** | 피싱, 보이스피싱 | 고객의 개인 인증정보가 외부에서 탈취되어 부정출금 발생 |
| **자금세탁 목적 거래** | 제3자 명의 이용 | 차명 계정 다수 생성 후 자금 분산 이체 시도 |
| **외부 해킹 공격** | 제휴 거래소 또는 지갑 해킹 | 외부 지갑에서 유출된 자산이 당사로 유입되며 추적 우회 시도 |
| **위장된 정상거래** | 믹서·토네이도캐시 활용 | 거래 경로를 은닉한 상태에서 자금세탁 시도 |
| **불완전한 KYC** | 허위 정보 등록 | 신분증 위조, 주소 위조 등을 통한 계정 생성 후 불법 거래 시도 |

#### 8.2 대응 절차

##### 이상 거래 실시간 감지 및 자동 보류

* + FDS(이상거래탐지시스템)를 통해 의심거래 자동 식별
  + 예시: 출금 주소 다수 분산, 첫 입금 후 즉시 전액 출금 등
  + 해당 거래 자동 보류 및 AML 팀에 즉시 알림

##### 고객 계정 정지 및 확인 요청

* + 사고 계정에 대해 즉시 **입출금 정지 및 본인확인 요청**
  + 고객의 정당한 요청이 아닐 경우 사고 접수 처리 및 자산 보호

##### 의심거래 보고(SAR) 제출

* + 관련 내역을 금융정보분석원(FIU)에 의심거래보고(SAR) 형태로 제출
  + 거래 시점, 계정 정보, 자산 종류, 경유된 외부 지갑 주소 등을 포함

##### 외부 기관 및 제휴사 공조

* + 필요 시 경찰청 사이버수사대, 외부 거래소, 블록체인 분석 업체와의 협조
  + 자산 추적 및 회수 가능성 검토

##### 피해 고객 보호 절차 진행

* + 필고객이 입은 손해 최소화를 위한 신속 조치
  + 피싱 피해 확인 시 경찰 수사 협조 문서 요청 후 보상/환급 여부 검토

#### 8.3 재발 방지를 위한 제도화 방안

##### 이상거래탐지 시스템(FDS) 고도화

* + 자산 종류별, 고객 유형별 이상 거래 패턴 DB 지속 업데이트
  + Mixer/Privacy 코인 관련 주소 블랙리스트 정기 갱신

##### 피싱 방지 위한 고객 대상 보안 교육 강화

* + 피싱·스미싱 사례 알림, 로그인/출금 시 보안 경고창 제공
  + OTP/MFA 의무 사용 적용 확대

##### 고위험 국가 및 주소 리스크 평가 강화

* FATF 고위험국가와 연계된 IP, 주소, 트랜잭션 경로 자동 차단

1. 계정 생성 단계 KYC 검증 강화
   * eKYC 도입, 위조 신분증 판별 솔루션 연계
   * AI 기반 문서 진위 검증 솔루션 적용

### **9. 위반 시 조치**

위반 행위는 해당자의 직위와 사안의 심각성에 따라 인사 조치, 징계, 해고 또는 수사기관 신고 조치를 포함한다.

### **10. 지침의 검토 및 개정**

* 본 지침은 연 1회 이상 검토되며, 관련 법률 및 기술 변화에 따라 필요 시 수시 개정할 수 있다.