월렛관련 업무지침

개정이력

|  |  |  |  |
| --- | --- | --- | --- |
| No. | 개정 사유 및 내용 | 개정일자 | 담당자 |
| 1.00 | 제정 | 2024.04.05 | 최철훈 |

목차

[목적 3](#_Toc69131067)

[범위 3](#_Toc69131068)

[제1조 (월렛룸) 3](#_Toc69131069)

[제2조 (월렛룸 내 작업) 3](#_Toc69131070)

[제3조 (월렛존) 3](#_Toc69131071)

[제4조 (외주개발존) 4](#_Toc69131072)

[제5조 (노드서버) 4](#_Toc69131073)

[제6조 (원격접근) 4](#_Toc69131074)

[제7조 (월렛구성) 5](#_Toc69131075)

[제8조 (콜드월렛 단말통제) 5](#_Toc69131076)

[제9조 (추가인증) 5](#_Toc69131077)

[제10조 (주요 직무자 점검) 6](#_Toc69131078)

[제11조 (주요 직무자 단말통제) 6](#_Toc69131079)

[제12조 (로그관리) 6](#_Toc69131080)

[제13조 (로그검토) 7](#_Toc69131081)

[제14조 (월렛행위확인) 7](#_Toc69131082)

[제15조 (소산백업) 7](#_Toc69131083)

[제16조 (개발요구사항) 7](#_Toc69131084)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사')의 핫월렛 및 콜드월렛 업무를 보호하기 위한 활동을 규정함으로써 회사의 안전한 월렛관리를 지속적으로 이루게 하는데 그 목적이 있다.

# 범위

회사의 월렛 운영 관련한 조직에 대하여 적용되며, 회사 내 다른 운영지침보다 본 월렛관련 업무지침이 우선시되어야 한다.

# 제1조 (월렛룸)

1. 콜드/핫 월렛 관련 보관, 월렛 사용을 위한 공간 등 월렛관련 중요공간을 일반업무에 대한 통제구역과 구분하여 별도 분리된 통제구역으로 지정한다.

2. 공통적인 보호구역 지정에 관련해서는 ST01(물리적 업무지침) - 제1조(보호구역 지정)를 준용한다.

# 제2조 (월렛룸 내 작업)

1. 통제구역으로 지정된 월렛룸(중요 월렛관련 운영 및 보관장소) 내 작업을 위해서는, 사전에 책임자의 승인을 통해 담당자 1인이 아닌 2인 이상이 함께 동반하여 업무를 처리하여야 한다.

2. 공통적인 보호구역내 작업에 관해서는 ST01(물리적 업무지침) - 제6조(보호구역내 작업)를 준용한다.

# 제3조 (월렛존)

1. 월렛 운영과 관련된 단말 및 시스템(월렛룸)은 별도의 네트워크 영역으로 구분하여야 한다.

2. 공통적인 네트워크 분리 관련해서는 ST03(접속통제관련 업무지침) - 제2조(네트워크 분리 및 접근통제)를 준용한다.

# 제4조 (외주개발존)

1. 가상자산거래서비스 또는 개인정보처리시스템을 외주개발 시, 외부인의 개발환경(전산설비 및 물리적 장소)과 내부업무용을 분리하여 운영하여야 한다.

2. 공통적인 네트워크 분리 관련해서는 ST03(접속통제관련 업무지침) - 제2조(네트워크 분리 및 접근통제)를 준용한다.

# 제5조 (노드서버)

1. 가상자산 노드서버와 분산원장을 동기화하는 취급업소의 노트서버는 내부망에 존재하여야 한다.

2. 가상자산 노드서버와 분산원장을 동기화하는 취급업소의 노드서버의 운영구조상 불가피하게 DMZ구간에 필수적으로 위치해야 하는 경우에는, 이로 인해 발생하는 위험요소(불특정 다수로 인한 외부공격을 받을 수 있는 가능성)에 대한 보완대책을 마련해야 한다.

3. 가상자산 노드서버와 분산원장을 동기화하는 취급업소의 노드서버의 운영구조상 불가피하게 DMZ구간에 필수적으로 위치해야 하는 경우에는, 경영진의 승인을 통해 진행한다.

4. DMZ 구간에 존재하는 노드서버와 분산원장을 동기화하는 취급업소의 노드서버에서는 개인키 및 개인키가 포함된 월렛을 사용하면 안된다.

5. 공통적인 암호화 관련해서는 ST05(운영관련 업무지침) - 제4조(암호화)를 준용한다.

# 제6조 (원격접근)

1. 외부네트워크를 통한 월렛 관련 시스템의 원격접근은 예외없이 금지한다.

2. 월렛 관련된 응용프로그램 운영구조상 외부망을 통해 원격접근이 필수적일 경우, 이로 인해 발생하는 위험요소(외부공격을 받을 수 있는 가능성 등)에 대한 보완대책을 마련하여야 한다.

3. 월렛 관련된 응용프로그램 운영구조상 외부망을 통해 원격접근이 필수적일 경우, 경영진의 승인을 통해 진행한다.

4. 공통적인 원격접근 관련해서는 ST03(접속통제관련 업무지침) - 제1조(원격지 접근시 보호대책)를 준용한다.

# 제7조 (월렛구성)

1. 취급하는 모든 가상자산에 대해 핫월렛과 콜드월렛을 사용해야 한다. 다만, 서비스 특성상 핫월렛을 사용하지 않을 경우에는 해당사항이 없다.

2. (법) 핫월렛과 콜드월렛이 처리하는 금액의 비율은 2:8로 운영하여야 한다. 다만, 서비스 특성상 핫월렛을 사용하지 않을 경우에는 해당사항이 없다.

3. 가상자산의 월렛(핫/콜드) 사용 시, 멀티시그 방식을 적용해야 한다. 만약, 멀티시그 방식을 적용할 수 없을 경우에는, 그에 준하는 방식(2인 이상의 MFA(Multi-Factor Authentication) 인증, 자체 개발한 멀티시그 기능(2개 이상의 key가 있어야만 거래가 가능하도록 통제 적용) 등)으로 적용하여야 한다. 다만, 서비스 특성상 핫월렛을 사용하지 않을 경우에는 콜드월렛에만 적용하면 된다.

# 제8조 (콜드월렛 단말통제)

1. 콜드월렛 전용단말기에 대해서는 네트워크 접속(인터넷 사용, 목적외 SW운영 등)을 차단하여야 한다.

2. 공통적인 인터넷 접속통제 관련해서는 ST03(접속통제관련 업무지침) - 제6조(인터넷 접속 통제)를 준용한다.

# 제9조 (추가인증)

1. 회원인 이용자의 로그인/출금/사용자정보변경 등의 서비스를 이용 시, 추가적인 인증수단(OTP, 인증서, 기기인증 등)을 통해 인증이 되도록 하여야 한다.

2. 이체 등 지갑관련한 주요 직무자(지갑전용단말기 사용자)에 대해서는 내부망에서 접속할 경우에도 추가적인 인증수단(OTP 등)을 적용해야 한다.

3. 공통적인 주요직무자 관리에 대해서는 ST04(접근제어관련 업무지침) - 제5조(주요 직무자 관리)를 준용한다.

# 제10조 (주요 직무자 점검)

1. 월렛관련 정보시스템(가상자산 노드서버, 키관리 시스템, 월렛서버, 월렛 관련 어플리케이션 등)의 일반 사용자 계정을 주요 직무자로 지정한다.

2. 월렛관련 정보시스템(가상자산 노드서버, 키관리 시스템, 월렛서버, 월렛 관련 어플리케이션 등)의 일반 사용자 계정 현황은 반기별로 자산 관리자가 점검한 후 정보보호관리자에게 보고한다.

3. 공통적인 주요 직무자 관리부분은 ST04(접근제어관련 업무지침) - 제5조(주요 직무자 관리)를 준용한다.

# 제11조 (주요 직무자 단말통제)

1. 내부 네트워크를 통해서 원격으로 이체 등 지갑관련한 주요업무 사용자 계정을 부여받은 해당 계정(지갑전용단말기 사용자)은 미리 지정한 특정 단말에서만 접근 가능하여야 한다.

2. 공통적인 원격접근 통제에 대해서는 ST03(접속통제관련 업무지침) - 제1조(원격지 접근시 보호대책)를 준용한다.

# 제12조 (로그관리)

1. 가상자산 거래기록 관련한 로그는 15년간 보관을 해야 한다.

2. 로그내 월렛관련 개인키, 암호화키, 패스프레이즈 등이 포함되지 않도록 한다. 만약, 월렛관련 개인키, 암호화키, 패스프레이즈 등이 로그에 포함될 경우에는 해당 로그를 암호화하여 보관한다.

3. 고객의 중요원장에 직접 접근하여 작업(조회·수정·삭제·삽입)한 경우, 해당 작업자 및 작업내용 등은 5년간 보관한다.

4. 공통적인 로그관리 관련해서는 ST06(로그관련 업무지침) - 제2조(정보시스템 로그기준)를 준용한다.

# 제13조 (로그검토)

1. 월렛과 관련된 정보시스템에 대한 사용자 접근이 업무상 허용된 범위에 있는지 월1회 이상 로그를 검토하여야 한다.

2. 공통적인 로그검토 관련해서는 ST06(로그관련 업무지침) - 제4조(로그검토)를 준용한다.

# 제14조 (월렛행위확인)

1. 핫월렛 운영과 관련하여 이상행위를 확인하여야 한다. (법) 특히, 가상자산시장을 개설/운영하는 가상자산사업자일 경우에는 이상거래를 상시 감시하여야 한다. 다만, 서비스 구성상 핫월렛을 사용하지 않을 경우에는 해당사항이 없다.

2. 핫월렛 업무행위가 다음 각목의 이상행위에 해당할 경우에는 담당자에게 알람 등을 통해 알려줘야 한다. 다만, 서비스 구성상 핫월렛을 사용하지 않을 경우에는 해당사항이 없다.

가. 월평균 처리 금액대비 3배의 금액이 처리되거나, 30분 이내에 일평균 처리 금액의 50%이상이 처리될 경우

나. 실시간/1시간/1일 별로 보유액 대비 90%/80%/70%의 이체가 실시간/1시간평균/1일평균 동안 발생될 경우

다. 평소 위치정보의 급격한 변화(국내->해외 등), 물리적 시간대비 위치정보의 급격한 변화(서울거래 후 1시간 후에 부산거래 등)가 발생될 경우

라. 사용자 프로필에 기반을 두어 평소 패턴이나 이용자 프로필에 맞지 않은 거래가 발생될 경우

마. 사용자 접속 단말기, OS 및 브라우져, IP정보 등의 환경정보가 변경될 경우

바. 출금계좌정보의 변경 등 계좌정보가 변경될 경우

2의2. 기존 이상거래에 대한 축적된 데이터를 기반으로 비정상 의심거래 탐지정책을 주기적으로 검토하여 적용해야 한다.

2의3. (법) 가상자산시장을 개설/운영하는 가상자산사업자일 경우에는 이상거래 상시 감시 중 법률에 의한 불공정거래행위가 의심되는 경우에는 지체없이 금융위원회 및 금융감독원장에게 통보하여야 한다. 또한, 불공정거래행위를 위반한 혐의가 충분히 확인된 경우에는 지체없이 수사기관에 신고하고 그 사실을 금융위원회 및 금융감독원장에게 보고하여야 한다.

3. 콜드월렛 운영과 관련한 계정의 업무행위에 대해서는 책임자가 이중 확인하여야 한다.

4. 공통적인 모니터링 관련해서는 ST08(관제관련 업무지침) - 제3조(네트워크 및 데이터흐름 모니터링)를 준용한다.

# 제15조 (소산백업)

1. 월랫운영과 관련된 데이터는 소산 백업하여야 한다. 특히, 월렛 암호화 키(프라이머리 키)의 백업본과 월렛 암호화 키의 패스프레이즈는 대표(대표 사망시 법적 상속자 포함)만 접근할 수 있는 소산장소(개인금고 등)에 보관해야하며, 해당 보관장소에 대해서는 멀티시그 분할키를 가지고 있는 사용자에게 공유해야 한다.

2. 공통적인 백업관련 해서는 ST06(로그관련 업무지침) - 제3조(보관 및 백업)를 준용한다.

# 제16조 (개발요구사항)

1. 월렛 관련 어플리케이션 개발 시 설계 단계에서부터 가상자산관련 보안 요구사항(멀티시그 적용여부, 가상자산 노드서버 운영, 거래결과 확인방법, 공인IP필요성, DMZ구간에 가상자산 노드서버 배치필요성, 불특정 IP/PORT 통신필요성 등)을 고려하여야 한다.

2. 공통적인 개발 보안요구사항은 ST07(개발관련 업무지침) - 제1조(개발 시 보안요구사항)를 준용한다.