접근제어 관련 업무지침

개정이력

|  |  |  |  |
| --- | --- | --- | --- |
| No. | 개정 사유 및 내용 | 개정일자 | 담당자 |
| 1 | 제정 | 2024.04.05 | 최철훈 |
|  |  |  |  |

목차

[목적 3](#_Toc13594233)

[범위 3](#_Toc13594234)

[제1조 (직무분리) 3](#_Toc13594235)

[제2조 (안전한 인증절차) 3](#_Toc13594236)

[제3조 (1인 1계정) 4](#_Toc13594237)

[제4조 (비밀번호) 5](#_Toc13594238)

[제5조 (주요 직무자 관리) 6](#_Toc13594239)

[제6조 (DBMS 접근통제) 7](#_Toc13594240)

[제7조 (비인가자 접근 통제) 7](#_Toc13594241)

[제8조 (응용프로그램 접근권한 제한) 8](#_Toc13594242)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사') 소유의 정보시스템에 대한 접근제어 관련한 업무에 대한 것으로 보다 안전하고 안정적인 정보시스템을 유지하기 위함이다.

# 범위

회사의 모든 임직원 및 외부 인력 들을 포함하여 회사의 정보시스템을 사용하는 자들로 정한다.

# 제1조 (직무분리)

1. 권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 주요 직무별 업무를 분리한다.

가. 개발/테스트 와 운영 분리

나. 운영과 감사 분리

2. 직무 분리가 어려운 경우 직무별 권한과 책임을 확인할 수 있도록 추가된 모니터링 등 보완통제를 시행할 수 있다.

# 제2조 (안전한 인증절차)

1. 모든 정보시스템에 접근시에는 ID, PW 방식 등의 사용자 인증을 통해 통제되어야 한다.

2. 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 알려야 한다.

3. 정보시스템별 사용자 계정 등록은 업무목적에 맞게 생성되며, 해당 정보시스템의 소속 부서장의 결재를 통해 진행된다. 단, 메인 백오피스의 사용자계정은 신입직원 입사시 자동으로 진행되며 별도의 계정 유효기간은 존재하지 않는다.

4. 임시 사용자 또는 외부자가 내부 정보시스템의 계정이 필요할 경우에는 정보시스템의 소속 부서장의 결재를 통해 진행이 되며, 이때 유효기간은 최대 3개월로 설정하며 필요시 유효기간 갱신을 통해 진행한다.

5. 임시 사용자 또는 외부자에게 접근권한을 부여해 줄 경우 보안서약서를 추가로 받아야 한다.

6. 정보시스템 사용자 계정의 삭제 또는 비활성화는 정보시스템의 소속 부서장의 결재를 통해 진행된다. 단, 직원의 퇴사 또는 계정 유효기간의 만료에 의한 경우에는 자동으로 처리된다.

7. 정보시스템 사용자 계정이 6개월 이상 미 사용시에는 계정비활성화 또는 삭제한다.

8. (법) 정보시스템별 계정의 접근권한 등록은 업무목적에 맞게 최소한으로 부여하며, 해당 정보시스템의 소속 부서장의 결재를 통해 진행한다. 단, 주요직무자(DBA, 개인정보취급자, 정보시스템의 최상위 권한자(이하 "정보시스템 관리자"라 한다), 특수권한(감사업무용자 등)는 정보보호책임자의 결재를 통해 진행한다.

9. 공식적인 계정 발급절차에 의해 정보시스템별로 발급받은 계정 사용자만이 정보시스템에 접근되어야 한다.

10. (법) 개인정보처리시스템에 접근 가능한 사용자는 승인된 개인정보취급자에 국한된어야 한다.

# 제3조 (1인 1계정)

1. (법) 정보시스템의 모든 사용자를 유일하게 구분할 수 있도록 정보시스템별 1인 1계정을 원칙으로 한다.

2. 정보시스템의 계정생성 시, 업무상 불가피하게 계정을 공유할 경우에는 그 사유와 타당성을 검토하고 해당 자산 책임자의 승인을 받아야 하고, 누가 공유계정을 사용했는지 확인할 수 있는 보완대책을 마련해야 한다.

3. 정보시스템의 계정 생성/수정/사용시 에는 추측 가능한 식별자를 사용해서는 안된다.

가. 신규 정보시스템 도입시 제조사 또는 판매사의 기본계정(root, admin, administrator 등)을 사용해서는 안된다. 단, 기존 시스템 구성상 불가피하게 사용해야 하는 경우에는 해당 자산 책임자의 승인을 받아야 한다.

나. 연속되는 숫자를 사용해서는 안된다.

다. 테스트, 회사명 등 쉽게 유추 가능한 것을 사용해서는 안된다.

# 제4조 (비밀번호)

1. (법) 사용자의 안전한 패스워드 사용 및 관리를 위해 다음과 같은 규칙을 따른다. 단, 시스템상에서 다음의 규칙을 제공하지 못할 경우에는 예외사항으로 처리할 수 있다.

가. 패스워드 생성 규칙

1) 3종류 8자리 이상 또는 2종류 10자리 이상으로 생성한다.

2) 동일한 문자 또는 숫자가 연속되는 것을 사용하지 않는다.

3) 계정명이 포함되지 않도록 한다.

4) 개인정보가 포함되지 않도록 한다.

5) 추측 가능한 패스워드는 사용하지 않도록 한다.

나. 패스워드 관리 규칙

1) 초기 패스워드 사용 시 최초 로그인 후 변경하여 사용하도록 한다.

2) 패스워드 변경은 반기별(6개월)로 실시한다. 단, 업무특성상 패스워드를 변경할 수 없는 상황 또는 6개월 이상을 사용해야 하는 경우가 존재할 경우에는 정보보호책임자의 승인을 통해 예외로 처리할 수 있다.

2. 고객, 회원 등 외부 이용자가 회사의 정보시스템 또는 웹서비스를 이용하고자 할 경우에는 다음과 같은 계정 및 패스워드 생성규칙을 따라야 한다.

가. 계정생성 규칙

1) 사용자 신상(주민등록번호, 회원번호 등)과 관련된 정보가 포함되지 않도록 한다.

2) 5자리 이상으로 생성한다.

나. 패스워드 생성 규칙

1) 2종류 8자리 이상으로 생성한다.

2) 동일한 문자 또는 숫자가 연속되는 것을 사용하지 않는다.

3) 계정명이 포함되지 않도록 한다.

4) 개인정보가 포함되지 않도록 한다.

5) 추측 가능한 패스워드는 사용하지 않도록 한다.

다. 패스워드 변경 규칙

1) 최대 6개월에 한번씩 패스워드를 변경하도록 유도한다.

3. 고객, 회원 등 외부 이용자가 회사의 정보시스템 또는 웹서비스를 이용하고자 회원가입 시 계정 및 패스워드 생성 규칙을 공지해야 한다.

# 제5조 (주요 직무자 관리)

1. DBA, 개인정보취급자, 정보시스템 관리자, 특수권한(감사업무용 등)사용자 등 중요정보를 대량으로 취급하는 임직원을 주요직무자로 지정한다.

2. 주요 직무자 지정의 최소화 등 적정성 여부를 담당 부서의 부서장이 반기 1회 검토 후 정보보호관리자에게 보고한다.

3. 정보시스템에 대한 관리자권한 및 망분리대상자에 대한 권한 부여현황은 반기별로 자산 관리자가 점검한 후 정보보호관리자에게 보고한다

4. 정보시스템에 대한 관리자 및 망분리대상자는 업무에 맞게 최소한으로 설정하여야 한다.

5. 서버에 로컬터미널이 아닌 원격으로 접근 시 안전한 접근수단(SSH 등)을 적용하여야 한다.

가. 서버의 OS내 계정 사용자에 대해서 내부망에서 접속할 경우에도 추가적인 인증수단(OTP 등)을 적용해야 함

나. 정보시스템의 관리자 계정에 대해서 내부망에 접속할 경우에도 추가적인 인증수단(OTP 등)을 적용해야 함

다. 이체 등 지갑관련한 주요업무 사용자 계정을 부여받은 해당 계정(지갑전용단말기 사용자)에 대해서 내부망에서 접속할 경우에도 추가적인 인증수단(OTP 등)을 적용해야 함

# 제6조 (DBMS 접근통제)

1. 데이터베이스의 접근을 허용하는 응용프로그램 현황 및 사용자별 직무현황을 최신으로 보유하여야 한다.

2. 데이터베이스에 접근하는 응용프로그램별로 데이터베이스 접근을 위한 사용자계정이 유일하게 구분할 수 있도록 식별자를 할당하여야 한다.

3. (법) 개인정보처리시스템과 연동되어 사용되는 DB의 접근 가능한 사용자는 승인된 개인정보취급자에 국한되어야 한다.

# 제7조 (비인가자 접근 통제)

1. 사용자 인증시 연속으로 로그인 실패 시에는 특정시간이 지난 이후에 재 로그인 시도를 할 수 있도록 해야 한다. 만약, 시스템적으로 특정시간동안 로그인 시도를 막을 수 없을 경우에는 예외로 할 수 있다.

2. 연속으로 로그인 실패시에는 불법 로그인 시도로 파악하여 해당 시스템 담당자에게 경고 안내를 보내야 한다. 만약, 시스템적으로 로그인 실패 시 경고메시지를 보낼 수 없을 경우에는 예외로 할 수 있다.

3. 사용자 접속 후 일정시간 사용이 없으면 연결을 종료(세션 타임아웃 시간 설정)하여야 한다.

# 제8조 (응용프로그램 접근권한 제한)

1. 응용프로그램의 동일 사용자 동시 세션수를 차단하여야 한다.

2. 개인정보를 다루는 응용프로그램의 사용자는 승인된 개인정보취급자에 국한되어야 한다.

3. 응용프로그램 별 계정의 접근권한 등록은 업무목적에 맞게 최소한으로 부여하며, 해당 응용프로그램의 관리소속 부서장의 결재를 통해 진행되어야 한다.