접속통제 관련 업무지침

개정이력

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

목차

[목적 3](#_Toc13593756)

[범위 3](#_Toc13593757)

[제1조 (원격지 접근 시 보호대책) 3](#_Toc13593758)

[제2조 (네트워크 분리 및 접근통제) 4](#_Toc13593759)

[제3조 (공개서버의 접근통제) 5](#_Toc13593760)

[제4조 (무선 네트워크 보호대책) 5](#_Toc13593761)

[제5조 (단말기/모바일기기 접속관리) 5](#_Toc13593762)

[제6조 (인터넷 접속 통제) 6](#_Toc13593763)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사') 소유의 정보시스템에 대한 네트워크 분리, 원격접근 시 보호대책, 업무용 단말기의 접근통제 등 네트워크 접속통제에 대한 것으로 보다 안전하고 안정적인 정보시스템을 유지하기 위함이다.

# 범위

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

# 제1조 (원격지 접근 시 보호대책)

1. 회사의 보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지한다.

2. 내부 네트워크를 통해서 원격으로 정보시스템을 관리하는 경우 관리자계정은 미리 지정한 특정 단말에서만 접근 가능하여야 한다.

가. 이체 등 지갑관련한 주요업무 사용자 계정을 부여받은 해당 계정(지갑전용단말기 사용자)에 대해서는 미리 지정된 특정단말에서만 접근할 수 있도록 해야 함

3. (법) 관리자 및 일반 사용자가 자택 등 외부망에서 회사의 개인정보처리시스템에 접속하고자 할 경우에는, 외부망에서 접근 시 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호 등 2펙터 인증)을 사용하여야 한다.

4. 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템에 접속하는 것은 원칙적으로 금지한다. 단, 업무상 부득이한 사유로 인해 허용하는 경우에는 다음과 같은 보호대책을 적용해야 한다.

가. 책임자로부터 승인

나. 안전한 접속수단(전용선, VPN 등)

다. 접속단말 보안(백신, 패치 등) 적용

라. 일정기간동안(최장 6개월) 접근이 가능하도록 기간관리

# 제2조 (네트워크 분리 및 접근통제)

1. 외부로부터의 접근이 불가피한 웹서버, 메일서버 등의 공개용 서버는 DMZ 영역에 위치시키고 공개서버를 경유하여 내부 업무망으로의 접근이 이루어지지 않도록 접근통제를 수행하여야 한다.

2. 외부 사용자에게 서비스를 제공하는 네트워크(외주서비스, 민원실, 교육장 등)는 내부 업무용 네트워크와 분리하여야 한다. 단, 업무상 불가피하게 외부 사용자가 내부 업무용 망에 접근을 해야 할 경우에는 내부망 관리통제를 동일게 적용받아야 한다.

3. 보안등급이 "기밀"로 분류된 데이터베이스는 별도의 네트워크 영역으로 구분하여야 한다.

4. 공개용 서버를 통해 내부 네트워크 침입이 불가능하도록 DMZ구간과 내부 네트워크를 분리하여야 한다.

5. 개발자의 비인가된 운영환경으로의 접근을 막기위하여 개발 및 시험 시스템을 운영시스템과 원칙적으로 분리하여야 한다.

6. 개발/테스트 존과 운영존은 물리적 및 논리적으로 분리되어야 하고, 관련업무자도 분리해야 한다. 다만, 개발/테스트에 참여한 사람이 해당 시스템/서비스의 운영업무를 동시에 진행해야만 할 경우에는 해당담당자에 대한 접근이력/변경이력 검토 및 정보보호책임자 승인 등 보완대책이 이루어져야 한다.

7. (법) 내부 네트워크에 대한 비인가 접근을 통제하기 위하여 정보시스템이 내부 네트워크에 접근 시 IP관리, 정보시스템 인증 등을 통해 장비에 대한 접근통제가 이루어져야 한다.

가. 단말기에 IP를 배정하여 관리

나. 배정된 단말기의 IP를 임의 변경 시 사용할 수 없도록 통제

# 제3조 (공개서버의 접근통제)

1. 웹서버의 DB접근은 제한된 IP와 포트로만 접근 제어되어야 한다.

# 제4조 (무선 네트워크 보호대책)

1. 무선랜 등을 통해 무선인터넷을 업무용으로 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 다음과 같은 보호대책을 수립하여 적용하여야 한다.

가. 사용자 인증: 맥인증

나. 송수신 데이터 암호화: WPA2, AES

다. SSID: 히든으로 숨김

라. 사용제한: 통제구역내에서는 사용할 수 없음

2. 비인가 무선 AP를 업무용으로 사용할 수 없음을 인지시켜야 한다.

# 제5조 (단말기/모바일기기 접속관리)

1. 회사 자산에 등록된 업무용 PC만 내부 네트워크에 연결되도록 하여야 한다.

2. 회사 자산이 아닌 PC를 내부 네트워크에 연결하고자 할 경우에는 자산책임자의 승인을 통해 업무용PC와 동일한 보호대책을 적용하여야 한다.

3. 업무용으로 사용하는 모바일기기를 네트워크에 연결할 경우 다음을 따라야 한다.

가. 회사 자산에 정식 등록되지 않은 모바일기기(핸드폰 등 통신모듈이 자체 내장된 모바일기기 포함)를 업무용으로 사용하는 것을 원칙적으로 금한다. 단, 유지보수 등을 위해 회사 자산에 정식 등록되지 않은 모바일기기를 통제구역에 반입하고자 할 경우에는 물리적보안지침을 따른다. 그리고, 임직원의 개인소유 모바일기기를 제한구역에 반입하는 것은 허용하나, 업무용으로는 사용할 수 없다.

나. 회사의 내부망에 접속하기 위해서는 맥 또는 IP인증 등을 받아야 한다.

다. 회사 자산에 정식 등록된 모바일기기는 내부 네트워크에서만 사용한다.

4. PC 및 노트북을 업무 목적으로 네트워크에 연결할 경우에는 다음과 같은 통제를 따라야 한다.

가. 공유폴더를 사용하지 못하도록 막는다.

나. 업무상 공유폴더가 필요한 경우 승인을 통해 1인1계정으로 접근하도록 한다.

다. 업무상 공유폴더가 필요한 경우 계정별로 패스워드를 설정하도록 한다.

라. 업무상 공유폴더가 필요한 경우 계정별로 접근권한을 최소한으로 설정하도록 한다.

5. 업무용으로 사용하는 모바일기기를 통해 정보시스템에 접근하지 않는다. 다만, 업무상 필요한 경우에는 사전 승인을 거쳐 최소한의 권한으로 접근될 수 있도록 한다.

6. PC, 모바일 기기 등 단말기기를 통한 정보시스템의 사용현황을 반기별(6개월)로 해당 정보시스템 담당자가 모니터링 후 해당 자산 책임자에게 보고한다.

7. 모바일 기기에 대한 다음의 내용에 대해 주기적인 점검을 진행한다.

가. 중요정보를 모바일 기기에 저장 시 암호화

나. 비밀번호 설정하여 운영

다. 안티바이러스 프로그램이 설치

# 제6조 (인터넷 접속 통제)

1. 보안등급이 "기밀"로 분류된 정보시스템에 대해, 고유 서비스를 제외한 모든 나머지 서비스는 차단되어야 한다.

2. (법) 법에서 정하는 망분리 대상 기업에 한해, 개인정보처리시스템에 접근하여 개인정보를 다운받거나, 파기하거나, 개인정보처리시스템의 접근권한을 변경할 수 있는 개인정보취급자에 대해 망분리를 해야 한다. 단, 클라우드 서비스를 사용하여 개인정보처리시스템을 구성할 경우 망분리 대상자는 해당 클라우드 서비스에 대한 접속 외에는 인터넷을 차단하는 것으로 망분리 적용을 갈음한다.

3. 망분리 대상자가 아닌 일반 정보시스템의 어드민관리자의 단말기에 대해서는 외부로 데이터를 전송할 수 있는 인터넷 서비스를 제한하여야 한다. 만약, 업무상 필요할 경우에는 사용기간을 정하여 해당 사용자가 속한 부서장의 승인을 통해 사용되어야 한다.

4. (법) 망분리 대상자가 아닌 일반 개인정보취급자의 단말기에 대해서는 외부로 데이터를 전송할 수 있는 인터넷 서비스를 제한하여야 한다.