관리사무소 업무 수행을 위한

# 공동주택 정보보호 가이드

2023. 10.

SK에코플랜트

정보보호담당

# ▪ 가이드 구성



[별첨 문서]

1. 홈네트워크 장비 보안설정 가이드 (3종)
2. 홈네트워크 장비 보안점검 체크리스트
3. 공동주택 개인정보보호 상담사례집 (개인정보위원회)

# 1. 배경 및 목적

## ▪ 배경

2021년 홈네트워크 시스템 해킹에 의한 세대 영상정보 유출 사고가 있었고, 이러한 해킹 사고의 예방과 보안 강화를 위해 2022년 7월 1일 이후 인허가 된 공동주택은『지능형 홈네트워크 설비 설치 및 기술기준』에 따라 세대간 망분리 등 법률적 보안요건 이행이 의무화 되었음.

## ▪ 가이드 배포 목적

SK에코플랜트는 본 가이드를 통하여 기 입주 단지의 해킹 사고의 예방과 보안 강화를 위해 필요한 최소한의 보호조치를 권고 하고, 일반적인 보안 관리에 도움이 될 수 있는 사항들을 같이 안내하여, 시공사로서 기 입주 단지의 보안수준을 개선하는데 도움을 제공 하고자 함.

## ▪ 요청 사항

홈네트워크 제조/운영사와 함께 본 가이드에 기술된 보호조치의 적용여부를 판단하여 보안사고를 예방할 것을 요청드림.

# 2. 유의사항

- 본 가이드는 모든 법률적 요구사항에 대해 기술하고 있지 않음. 따라서, 더 상세한 가이드 필요시 관계 법령 및 KISA에서 발행된『홈네트워크 보안가이드』또는 별첨『SK에코플랜트 홈네트워크 장비 보안설정 가이드 (3종)』를 참고할 것을 권장함.

- 홈네트워크 제조/운영사와 장애위험에 대한 충분히 검토 후 보호조치를 적용할 것을 권장함

# 3. 홈네트워크 시스템 보안 관리

## 3-1. 방화벽

| | | |
|---|---|---|
| 주요 예상 Risk | 1 | ✓ 외부에서 단지 방화벽의 관리자 페이지 접속이 가능하여, 방화벽에 대한 해킹사고 발생 (PW 무차별 대입공격 등) |
| | 2 | ✓ 방화벽 관리자 ID/PW가 유추하기 쉽게 설정되어 있어 [사례 1]과 조합되어 해킹사고 발생 (admin / abc123! 등) |
| | 3 | ✓ 방화벽에서 차단 없이, 외부에서 내부망에 존재하는 단지서버의 모든 서비스 포트로 접근 가능하여, 단지서버에 대한 해킹사고 발생 |
| | 4 | ✓ 장애 발생 우려, 네트워크 순간 단절 등에 대한 우려로 방화벽에 대한 최신 업데이트를 적용하지 않아 해킹사고 발생 |

**준수 사항**

**1. 방화벽 관리자 페이지는 외부 접속이 불가하도록 설정 필요**

- 원격 유지보수 필요 시, 허용이 필요한 특정 IP에 한하여 접속 가능하도록 설정
- 동시 로그인 제한, 인증 실패 임계치 적용(10회 이하), 타임아웃 설정(30분)

**2. 방화벽의 기본 ID는 변경하여 사용하며, PW는 유추하기 어렵도록 설정 필요**

- ID : 제조사 기본 ID(공장 출고 시 기본 설정되어 있는 ID)는 변경하여 사용
- PW : 영문, 숫자, 특수기호 조합 8자리 이상, 연속된 문자열 금지, OTP 추가 적용 등

**3. 방화벽 정책 (Rule-set) 적용 시 불필요하게 모든 IP 대역을 접속 허용하지 않도록 설정하고, 주기적으로 방화벽 정책 점검 필요**

- [출발지 : Any → 목적지 : 단지서버] 등 외부 어디에서나 접근 가능한 정책 제거

**4. 지속적인 유지보수를 통해 최신 버전 유지 필요**

- 유지보수 업체와 충분한 협의 및 장애대응 방안을 마련하여 최신 업데이트 수행

# 3. 홈네트워크 시스템 보안 관리

## 3-2. 단지 서버

**주요 예상 Risk**

| | |
|---|---|
| 1 | ✓ 단지 네트워크內 어디에서나 단지서버의 관리자 콘솔(SSH, RDP 등) 접속이 가능하여, 단지서버에 대한 해킹사고 발생 |
| 2 | ✓ 단지서버 관리자 ID/PW가 유추하기 쉽게 설정되어 있어 [사례 1]과 조합되어 해킹사고 발생 (root / abc123! 등) |
| 3 | ✓ 단지서버에 불필요한 서비스가 실행 중이거나 및 S/W가 설치되어 있어 관련 취약점으로 인한 해킹사고 발생 |
| 4 | ✓ 단지서버에 설치된 악성코드로 인해, 서버가 장악되어 정보유출 및 2차 해킹에 활용되는 사고 발생 |

**준수 사항**

**1. 서버 관리자 콘솔(SSH, RDP 등)에 비인가자의 접속이 불가하도록 설정 필요**

- 유지보수용 PC의 IP 에 한하여 접속 가능하도록 설정
- 동시 로그인 제한, 인증 실패 임계치 적용(10회 이하), 타임아웃 설정(30분)

**2. 기본 ID는 변경하여 사용하며, PW는 유추하기 어렵도록 설정 필요**

- ID : 제조사 기본 ID(공장 출고 시 기본 설정되어 있는 ID)는 변경하여 사용
- PW : 영문, 숫자, 특수기호 조합 8자리 이상, 연속된 문자열 금지 등
  (관리자 전용 웹 사이트 및 DB 관리 콘솔도 동일)

**3. 홈네트워크 서비스와 무관한 불필요 서비스 및 S/W 제거 필요**

- IIS, FTP, TELNET 등 OS 설치 시 자동 활성화 되는 불필요 서비스 제거
- Office, VNC, TeamViewer, 메신저 등 불필요(고위험) S/W 제거

**4. 서버 백신 설치 및 최신 보안 업데이트 유지 필요**

- 악성코드 감염/실행을 막기 위해 서버 백신을 설치하고, 최신 보안 업데이트 설치
- 악성코드로 인한 원격제어, 정보유출 방지를 위해 서버의 인터넷 접속 차단 (권장)
  : 타 시스템 연동 등 접속이 필요한 IP에 한하여 통신 허용 설정

# 3. 홈네트워크 시스템 보안 관리

## 3-3. 시스템 관리용 PC

| | | |
|---|---|---|
| 주요 예상 Risk | 1 | ✓ PW가 설정되어 있지 않은 관리용 PC에 비인가자가 로그인 |
| | 2 | ✓ 개인의 편의를 목적으로 관리용 PC의 PW를 Post-it 등에 기재 후 모니터에 부착하여 비인가자에 PW 노출 |
| | 3 | ✓ 인터넷 서핑을 통해 랜섬웨어 등 악성코드가 감염되어 동일한 네트워크內에 존재하는 다른 서버/PC에 악성코드 전파 |

**준수 사항**

**1. PW는 유추하기 어렵도록 설정 필요 (PW 미 설정 절대 금지)**

- 영문, 숫자, 특수기호 조합 8자리 이상, 연속된 문자열 사용 금지 등
- 화면보호기(10분 이내 잠김 설정)를 적용하여, 자리 이석 시 비인가 접근 방지

**2. PW 노출 방지 활동 필요**

- 메모 부착 및 동일한 PW의 반복사용 금지, 주기적 PW 변경 수행 (분기 1회)

**3. 악성코드 감염 방지 활동 필요**

**- 시스템 운영 업무와 무관한 인터넷 사용 금지**

: 업무적 사용의 경우에도 인터넷 접속 최소화 및 신뢰할 수 있는 사이트만 접속

: 시스템 관리용 PC의 인터넷 차단 (권장)

**- 시스템 운영 업무와 무관한 S/W 설치 금지**

: 파일공유(P2P), 메신저, 게임 등

**- 백신 설치 및 실시간 감시 활성화**

: V3등 백신 미보유시, Windows 바이러스 및 위협방지 기능 활성화로 대체 가능

**- 최신 보안 업데이트 유지**

: Windows 자동 업데이트 설정 권장

# 4. 관리사무소 보안 관리

## 4-1. 유/무선 네트워크 구성

| | | |
|---|---|---|
| **주요 예상 Risk** | 1 | ✓ 관리사무소 직원 업무용 PC의 월패드 네트워크 연결/사용으로 업무용 PC를 경유한 해킹 피해 및 악성코드 전파 위험 노출 |
| | 2 | ✓ 관리사무소 네트워크 유무선 공유기의 보안설정 미흡으로 비인가자의 관리사무소 네트워크 접근 가능 |

**준수 사항**

**1. 관리사무소 직원용 네트워크 별도 구성 필요**

- 월패드 네트워크와 분리되어 있는 별도의 인터넷 회선 구성
- 홈네트워크 시스템 운영과 무관한 직원 업무용 PC는 월패드 네트워크 연결 금지

**2. 네트워크 장비 보안설정 관리 필요**

**- 유무선 공유기 기본 관리자 ID 변경하여 사용**

: admin 등 제품 출고 시 설정되어 있는 기본 ID는 신규 ID로 변경하여 사용

**- 유무선 공유기 관리자 PW는 유추하기 어렵도록 설정**

: 영문, 숫자, 특수기호 조합 8자리 이상, 연속된 문자열 사용 금지 적용 등

**- 무선 네트워크 사용 시 안전한 인증/암호화 방식 설정**

: 인증 방식은 WPA2(혹은 WPA-PSK2) 이상 이용

: 암호화 방식는 AES나 CCMP(혹은 AES-CCMP) 이용

**- 최신 업데이트 상태 유지**

: 주기적으로 유무선 공유기의 Firmware 버전 확인 및 업데이트

**- 인가된 사용자만 사용할 수 있도록 설정 (권장)**

: PC의 MAC Address를 사전 등록하고, 등록되지 않은 PC는 차단

※ 사용중인 장비의 제조사 매뉴얼을 참고하여 상세한 설정방법을 확인/조치하거나 장비 관리 업체에 요청하여 개선 조치 진행 필요

# 4. 관리사무소 보안 관리

## 4-2. 개인정보 보호

✓ **개인정보란?** **'살아있는 개인'에 관한 정보로서 개인을 알아볼 수 있는 정보임**

- (그 자체로) 개인을 알아볼 수 있는 정보 (e.g : 이름, 주민등록번호, 영상정보 등)
- 다른 정보와 쉽게 결합하여 특정 개인을 알아 볼 수 있는 정보 (e.g : 주소, 직장, 전화번호 등)

✓ **관리사무소에서 취급하는 개인정보는?**

- ① 입주민 정보, ② 단지내 근무자 정보, ③ 방문객 정보 등

**※ 입주자 개인정보 보호 조치 등 공동주택 내 개인정보 관리/강화 방안은 『공동주택 개인정보보호 상담사례집』 참고**

**준수 사항**

**수집**

- **개인정보를 수집할 때는 정보주체의 동의를 받아야 함**
  - 법적 고지사항 4가지 안내 필요
    : ①목적, ②항목, ③보유기간, ④동의 거부 시 불이익

**이용**

- **동의 받은 목적으로만 이용 가능**
  - 수집 시 동의 받은 목적 外 사용 불가

**저장**

- **개인정보 문서는 안전하게 보관해야 함**
  - 온라인 문서 (파일)
    : 비밀번호 설정 등 암호화 하여 보관
  - 오프라인 문서 (출력물)
    : 시건 장치가 있는 캐비닛 또는 문서고에 보관

**파기**

- **보유 기간 및 목적 달성 시 지체없이 파기해야 함**
  - 목적 달성 후 영업일 기준 5일 이내
  - 온라인 문서 (파일) : 완전 삭제 (휴지통 비우기 등)
  - 오프라인 문서 (출력물) : 파쇄 (파쇄기)

# 4. 관리사무소 보안 관리

## 4-3. 정보보호 실천 사항

**준수 사항**

● **생활 속 (개인) 정보보호 실천 사항**

회사 지급 PC 사용
1인 1계정 사용


주기적인 PW 변경
작성규칙 준수

화면보호기 설정


불필요한 사이트
접속 금지

회의 후 회의자료 회수
화이트보드 지우기

활용이 끝난 문서 파쇄
(개인정보 등)

노트북 안전 보관
(시건 케이블 등)

퇴근 시 Clean Desk 및
개인 서랍 잠그기

# 4. 관리사무소 보안 관리

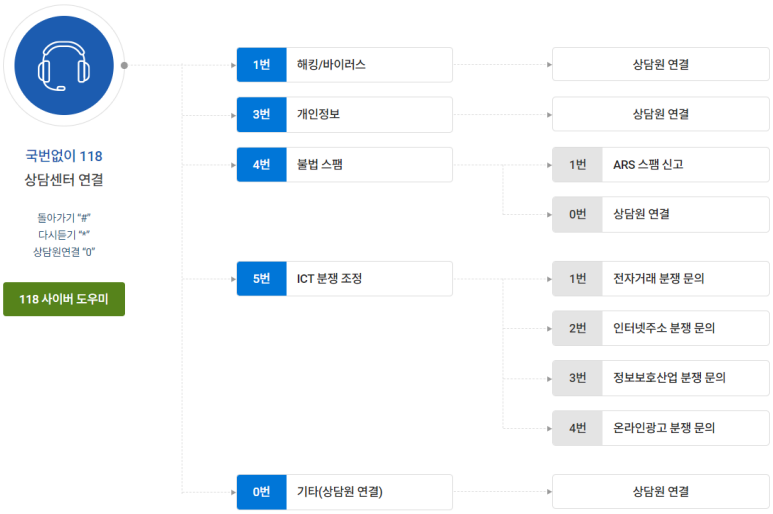
## 4-4. 보안사고 신고

**신고 접수처**

**사이버 침해사고 (종합)**

✓ **KISA(한국인터넷진흥원) 사이버 침해 대응 본부**

- **전화 : 국번없이 118**




**개인정보 침해사고 신고 및 상담**

✓ **KISA(한국인터넷진흥원) 개인정보침해신고센터**

- **전화 : 국번없이 118**
- 이메일 : privacyclean@kisa.or.kr
- 인터넷 : https://privacy.kisa.or.kr

**사이버 범죄 신고 및 상담**

✓ **경찰청 사이버 수사국**

- **전화 : 국번없이 182**
- 인터넷 : http://ecrm.cyber.go.kr