[**SK 헬스 서비스 클라우드 전환 정보보안 컨설팅 프로젝트**]

**보안요건 이행점검 보고서**

version 0.1.1

**문서 이력**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **버전** | **변경일** | **변경 내용** | **작성자** | **검토자** |
| 0.0.1 | 2022.06.07 | 보고서 초안 작성 | 도규탁 | 김백현 |
| 0.0.2 | 2022.06.08 | 보고서 초안 수정 | 도규탁 | 김백현 |
| 0.0.3 | 2022.06.09 | 보고서 초안 완료 | 고해준, 도규탁 | 김백현 |
| 0.1.0 | 2022.06.10 | 보고서 목차 수정 | 도규탁 | 백성광 |
| 0.1.1 | 2022.6.10 | 점검결과 내용 작성 | 고해준, 도규탁 | 김백현 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

목차

[Ⅰ. 개요 3](#_Toc105747837)

[1. 목적 및 배경 3](#_Toc105747838)

[2. 점검 일정 3](#_Toc105747839)

[3. 점검 인력 3](#_Toc105747840)

[4. 점검 방법(수행 절차) 3](#_Toc105747841)

[5. 점검 기준 4](#_Toc105747842)

[6. 진단 대상 5](#_Toc105747843)

[Ⅱ. 점검결과 7](#_Toc105747844)

[1. 점검결과 요약 7](#_Toc105747845)

[2. 점검결과 상세 8](#_Toc105747846)

[2.1 계정 권한 관리 8](#_Toc105747847)

[2.2 식별 인증 13](#_Toc105747848)

[2.3 접근통제 16](#_Toc105747849)

[2.4 암호화 적용 25](#_Toc105747850)

[2.5 로깅 및 모니터링 26](#_Toc105747851)

[2.6 보안관리 29](#_Toc105747852)

[2.7 개인정보보호 33](#_Toc105747853)

# **Ⅰ. 개요**

## 목적 및 배경

SK 헬스 서비스를 AWS 클라우드 환경에서 운영할 때 ISMS-P와 법률을 만족시키는 보안 요구사항 측면에서 이행 여부를 점검한다. 이를 통해 보안 요구사항들이 충족•불충족한지 식별하고 대책을 수립하는 데 목적이 있다.

## 점검 일정

2022년 06월 08일부터 2022년 06월 xx일까지 xx일 간 수행하였다

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **분류** | **내용** | **2022. 06.** | | | |
| **06. 08** | **06. 09** | **06. 10** | **06. 13** |
| **사전 준비** | 대상 범위 협의, 점검 방법 결정 |  |  |  |  |
| **이행 점검** | 점검 대상의 AWS 환경 구축 |  |  |  |  |
| 보안 요건 충족 여부 확인 |  |  | |  |
| **분석•평가** | 결과 보고서 작성 및 리뷰 |  |  |  |  |

[표 1] 점검 일정

## 점검 인력

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **이름** | **소속** | **파트** | **담당 업무** | **비고** |
| 고해준 | 1조 핼쑥해요 | 아키텍트 |  |  |
| 도규탁 | 1조 핼쑥해요 | 컴플라이언스 |  |  |

[표 2] 점검 인력

## 점검 방법(수행 절차)

1. **현황분석**

* 보안 요건 현황 파악
* AWS 클라우드 서비스 파악

1. **실사 점검**

* 점검 대상 AWS 클라우드 구축 환경 실사 점검 .

1. **충족/미충족 평가**

* 문제점 도출/원인분석
* 보안 요건 항목 충족/미충족 평가

1. **개선방안 제시**

* 충족되지 않은 요건 보안 설정 가이드 제시

**현황분석**

보안 요건 점검 대상들을 파악하고, AWS 클라우드에서 제공하는 보안 서비스(eg. WAF, Network Firewall, Cloud Watch 등)들에 대해 전반적으로 분석한다.

**실사점검**

AWS 클라우드 구축 환경을 실사하여 보안 요건 항목들을 점검한다.

**충족/미충족 평가**

AWS 클라우드 구축 환경을 실사한 것을 분석하여 보안요건을 충족 여부를 판단한다.

**개선방안 제시**

충족/미충족 평가를 통해 도출된 항목들에 대해서 보안 설정 가이드를 제시한다.

## 점검 기준

법률과 ISMS-P 인증의 기술적 보호조치 항목을 분류하여 보안요건 정의서를 작성하였고, 이를 기준으로 보안요건정의 항목들이 AWS 클라우드 환경에서 충족하는지 점검을 이행한다.

|  |  |  |
| --- | --- | --- |
| **법** | **시행령** | **고시** |
| 개인정보 보호법 | 개인정보 보호법 시행령 | 개인정보의 기술적 ·관리적 보호조치 |
| 개인정보의 안정성 확보 조치 |
| 정보통신망법 | 정보통신망법 시행령 | 정보보호조치에 관한 지침 |
| 위치정보법 | 위치정보법 시행령 | - |
| 클라우드 컴퓨팅법 | - | 클라우드 컴퓨팅서비스 정보보호에 관한 기준 |

법률: SK헬스 서비스의 인프라 단계에서 개인정보 및 중요정보 보호를 위해 준수해야 할 법률

[표 3] 법률 분류 항목

ISMS-P: 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷 진흥원 또는 인증기관이 증명하는 제도를 기술적 보호조치 항목으로 분류

|  |  |  |
| --- | --- | --- |
| **통합인증** | **분야 (인증기준 개수)** | |
| 관리 체계 수립 및 운영(16) | 1.1 관리체계 기반 마련(6) | 1.3 관리체계 운영(3) |
| 1.2 위험관리(4) | 1.4 관리체계 점검 및 개선(3) |
| 보호대책 요구사항(64)  개인정보 처리단계별  요구사항(22) | 2.1 정책, 조직, 자산 관리(3) | 2.7 암호화 적용(2) |
| 2.2 인적보안(6) | 2.8 정보시스템 도입 및 개발 보안(6) |
| 2.3 외부자 보안(4) | 2.9 시스템 및 서비스 운영관리(7) |
| 2.4 물리보안(7) | 2.10 시스템 및 서비스 보안관리(9) |
| 2.5 인증 및 권한 관리(6) | 2.11 사고 예방 및 대응(5) |
| 2.6 물리통제(7) | 2.12 재해복구(2) |
| 개인정보 처리단계별  요구사항(22) | 3.1 개인정보 수집 시 보호조치(7) | 3.3 개인정보 제공 시 보호조치(3) |
| 3.2 개인정보 보유 및 이용 시 보호조치(5) | 3.4 개인정보 파기 시 보호조치(4) |
|  | 3.5 정보주체 권리보호(3) |

[표 4] ISMS-P기준 항목

|  |  |  |
| --- | --- | --- |
| **통합인증** | **보호조치 분류** | **개수** |
| ISMS-P 인증항목  (102개) | 관리적 보호조치 항목 | 60개 |
| 물리적 보호조치 항목 | 8개 |
| **기술적 보호조치 항목** | **34개** |

[표 5] ISMS-P 보호조치 분류 항목

## 점검 대상

보안요건정의서에서 요구하는 항목들을 나타내고 있으며, 상세 현황은 다음과 같다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **보안코드** | **영역** | **세부영역** | **항목명** | **점검결과** | **비고** |
| Sec101 | 계정∙권한 관리 | 사용자 계정 관리 | 개인정보 및 중요정보에 대한 비인가 사용자 접근 권한 설정 | 충족 |  |
| Sec102 | 특수 계정 및  권한 관리 | 특수 계정의 권한 식별 및 관리 | 충족 |  |
| Sec103 | 계정 비밀번호  관리 | 사용자 및 관리자 계정 비밀번호 관리 | 충족 |  |
| Sec104 | 접근권한 검토 | 사용자 계정의 접근 권한 이력 점검 | 충족 |  |
| Sec105 | 보안시스템 관리 | 예외 정책 사용자 권한 관리 | 미충족 |  |
| Sec201 | 식별∙인증 | 사용자 인증 | 사용자 접근에 대한 인증 수단 적용 | 충족 |  |
| Sec202 | 외부 접근 사용자 인증 | 외부 접근에 대한 사용자 인증 | 충족 |  |
| Sec203 | 사용자 식별 | 사용자 계정 식별자 할당 | 충족 |  |
| Sec301 | 접근 통제 | 네트워크 접근 | 네트워크 비인가 사용자 접근 통제 | 충족 |  |
| Sec302 | 네트워크 영역 분리 및 통제 | 충족 |  |
| Sec303 | 외부 네트워크 접근통제 | 충족 |  |
| Sec304 | 무선 네트워크 접근통제 | 미충족 |  |
| Sec305 | 정보시스템 접근 | 정보시스템에 대한 접근수단 정의 및 접근통제 | 충족 |  |
| Sec306 | 정보시스템 접근에 대한 사용자 인증 통제 적용 | 충족 |  |
| Sec307 | 정보시스템 접속 차단 | 충족 |  |
| Sec308 | 서비스에 따른 독립된 서버 운영 | 충족 |  |
| Sec309 | 정보시스템 관계 없는 서비스 차단 | 충족 |  |
| Sec310 | 응용프로그램  접근 | 응용프로그램 접근 권한 제한 | 충족 |  |
| Sec311 | 응용프로그램 중요정보의 노출 최소화 | 미충족 |  |
| Sec312 | 응용프로그램 세션 관리 | 충족 |  |
| Sec313 | 관리자 전용 응용프로그램 비인가자 접근 통제 | 미충족 |  |
| Sec314 | 데이터베이스  접근 | 데이터베이스 접근통제 | 충족 |  |
| Sec315 | 원격접근 통제 | 단말기 접근통제 | 미충족 |  |
| Sec316 | 인터넷 접속 통제 | 외부 인터넷 접속 통제 | 충족 |  |
| Sec317 | 망분리 적용 및 통제 | 충족 |  |
| Sec318 | 보안시스템 통제 | 보안시스템 비인가자 접근 통제 | 미충족 |  |
| Sec401 | 암호화  적용 | 중요정보 암호화 | 개인정보 및 주요정보에 대한 암호화 적용 | 충족 |  |
| Sec402 | 암호키 관리 | 암호키 접근권한 관리 | 충족 |  |
| Sec403 | 비밀번호 암호화 | 비밀번호 암호화 적용 | 충족 |  |
| Sec501 | 로깅 및 모니터링 | 로그 관리 | 로그 기록 보관 및 관리 | 충족 |  |
| Sec502 | 로그 기록 접근권한 설정 | 충족 |  |
| Sec503 | 정보시스템 이상징후 인지를 위한 모니터링 절차 이행 | 충족 |  |
| Sec504 | 로그 시간 동기화 | 충족 |  |
| Sec505 | 이상행위 발생 시 신속한 분석 및 점검 | 충족 |  |
| Sec601 | 보안 관리 | 시험과 운영 환경 분리 | 시험 시스템과 운영시스템의 분리 | 미충족 |  |
| Sec602 | 시험 데이터 보안 | 실제 운영 데이터의 사용 제한 | 미충족 |  |
| Sec603 | 장애 관리 | 정보시스템의 장애 관리 | 충족 |  |
| Sec604 | 클라우드 보안 | 클라우드 서비스 보안 통제 정책 이행 | 충족 |  |
| Sec605 | 클라우드 서비스 관리자 권한 보호대책 적용 | 충족 |  |
| Sec606 | 공개서버 보안 | 공개서버 DMZ 설치 및 보안시스템 보호 | 충족 |  |
| Sec607 | 패치관리 | 공개 인터넷 접속을 통한 패치 제한 | 충족 |  |
| Sec608 | 악성코드 통제 | 악성코드 보호대책 이행 | 충족 |  |
| Sec609 | 악성코드 대응절차 이행 | 충족 |  |
| Sec610 | 취약점 점검 및 조치 | 최신 보안 취약점 분석 및 조치 | 미충족 |  |
| Sec701 | 개인정보보호 | 개인정보보호 | 개인정보처리시스템 법률 준수 검토 및 관리 | 충족 |  |

[표 6] 보안요건정의서 항목 리스트

점검 결과 항목

보안요구사항 점검 이행을 통해 점검 대상의 수준을 파악하여 충족, 미충족으로 분류한다.

|  |  |  |
| --- | --- | --- |
| **수준** | **보안 상태** | **비고** |
| **충족** | AWS클라우드 환경에서 보안 요건을 이행함 |  |
| **미충족** | AWS 클라우드 환경에서 보안 요건을 이행하지 않거나 이행할 수 없음 |  |

[표 7] 점검 결과 항목

# **Ⅱ. 점검결과**

## 점검결과 요약

## 점검결과 상세

### 2.1 계정 권한 관리

**사용자 계정 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec101 | **이행결과** | 충족 |
| **분류** | 사용자 계정 관리 | 미 충족 |
| **항목명** | 개인정보 및 중요정보에 대한 비인가 사용자 접근 권한 설정 | | |
| **요구사항 내용** | 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성‧등록‧변경 시 직무 별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가? | | |
| **이행 점검**  **내용** | * 직무 별 계정 그룹 분리 이행   **C:\Users\user\Downloads\KakaoTalk_20220608_160321112.png**   * 직무 별 계정 접근 권한 부여 이행   **C:\Users\user\Downloads\KakaoTalk_20220608_155701711.png** | | |
| **비고** |  | | |

**특수 계정 및 권한 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec102 | **이행**  **결과** | **충족** |
| **분류** | 특수 계정 및 권한 관리 | 미 충족 |
| **항목명** | 특수 계정의 권한 식별 및 관리 | | |
| **요구사항 내용** | 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리하고 있는가? | | |
| **이행**  **점검 내용** | * Admin 계정 권한 식별 및 관리 이행   C:\Users\user\Downloads\image.png | | |
| **비고** |  | | |

**계정 비밀번호 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec103 | **이행**  **결과** | 충족 |
| **분류** | 계정 비밀번호 관리 | 미 충족 |
| **항목명** | 사용자 및 관리자 계정 비밀번호 관리 | | |
| **요구사항 내용** | 사용자, 관리자 계정을 안전한 비밀번호를 설정하여 관리하고 있는가? | | |
| **이행**  **점검 내용** | * IAM을 통해 계정 비밀번호 정책 설정 이행      * Cognito를 통해 비밀번호 강도 정책 설정 이행 완료 | | |
| **비고** |  | | |

**접근권한 검토**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec104 | **이행**  **결과** | 충족 |
| **분류** | 접근권한 검토 | 미 충족 |
| **항목명** | 사용자 계정의 접근 권한 이력 점검 | | |
| **요구사항 내용** | 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성‧등록‧부여‧이용‧변경‧말소 등의 이력을 점검하고 있는가? | | |
| **이행**  **점검 내용** | 충족 | | |
| **비고** | **..** | | |

**보안 시스템 관리**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec105 | **이행**  **결과** | 충족 |
| **분류** | 보안시스템 관리 | **미 충족** |
| **항목명** | 예외 정책 사용자 권한 관리 | | |
| **요구사항 내용** | 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가? | | |
| **이행**  **점검 내용** | 예외 정책이 뭔지 몰라서..? | | |
| **비고** |  | | |

### 2.2 식별 인증

**사용자 인증**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec201 | **이행**  **결과** | **충족** |
| **분류** | 사용자 인증 | 미 충족 |
| **항목명** | 사용자 접근에 대한 인증 수단 적용 | | |
| **요구사항 내용** | 정보시스템 및 개인정보처리시스템에 대한 접근 시 사용자 인증 수단(인증서, OTP등)을 사용하고 있는가? | | |
| **이행**  **점검 내용** | * IAM에 있는 MFA 추가 인증을 통해서 사용자 인증 수단을 제공 이행 | | |
| **비고** |  | | |

**외부 사용자 인증**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec202 | **이행**  **결과** | 충족 |
| **분류** | 외부 접근 사용자 인증 | 미 충족 |
| **항목명** | 외부 접근에 대한 사용자 인증 | | |
| **요구사항 내용** | 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증 수단 또는 안전한 접속 수단을 적용하고 있는가? | | |
| **이행**  **점검 내용** | * Client VPN을 통해 외부에서 Bastion HOST에 대한 접속 수단 적용 이행 | | |
| **비고** |  | | |

**사용자 식별**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec203 | **이행**  **결과** | 충족 |
| **분류** | 사용자 식별 | 미 충족 |
| **항목명** | 사용자 계정 식별자 할당 | | |
| **요구사항 내용** | 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 있는가? | | |
| **이행**  **점검 내용** | * Cognito를 통해 사용자에 대한 식별자를 할당 적용 이행 | | |
| **비고** | **.** | | |

### 2.3 접근통제

**네트워크 접근**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec301 | **이행**  **결과** | **충족** |
| **분류** | 네트워크 접근 | 미 충족 |
| **항목명** | 네트워크 비인가 사용자 접근 통제 | | |
| **요구사항 내용** | 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가? | | |
| **이행**  **점검 내용** | * VPC의 NACL에서 SSH 접근에 대한 사용자를 제한한다.. * SSH의 인바운드 소스에는 개발자나 운영자 등 인가된 사용자의 IP 주소를 지정한다. | | |
| **비고** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec302 | **이행**  **결과** | 충족 |
| **분류** | 네트워크 접근 | 미 충족 |
| **항목명** | 네트워크 영역 분리 및 통제 | | |
| **요구사항 내용** | 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 통제하고 있는가? | | |
| **이행**  **점검 내용** | * VPC에서 서브넷 영역을 논리적으로 분리하여 통제한다. | | |
| **비고** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec303 | **이행**  **결과** | 충족 |
| **분류** | 네트워크 접근 | 미 충족 |
| **항목명** | 외부 네트워크 접근통제 | | |
| **요구사항 내용** | 데이터베이스 서버 등 중요 시스템이 외부와의 연결을 필요로 하지 않은 경우 사설 IP로 할당하여 외부 IP 접근통제 하고 있는가? | | |
| **이행**  **점검 내용** | * VPC를 통해 웹 서버, 데이터베이스 등에 A클래스 대역의 IP를 할당하여 접근통제 한다. | | |
| **비고** | **..** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec304 | **이행**  **결과** | 충족 |
| **분류** | 네트워크 접근 | 미 충족 |
| **항목명** | 무선 네트워크 접근통제 | | |
| **요구사항 내용** | 무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화 등 무선 네트워크 보호대책을 적용하고 통제하고 있는가? | | |
| **이행**  **점검 내용** |  | | |
| **비고** | **..** | | |

**정보시스템 접근**

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec305 | **이행**  **결과** | 충족 |
| **분류** | 정보시스템 접근 | 미 충족 |
| **항목명** | 정보시스템에 대한 접근 수단 정의 및 접근통제 | | |
| **요구사항 내용** | 서버, 네트워크시스템, 보안시스템 등 정보시스템 별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하고 있는가? | | |
| **이행**  **점검 내용** | * IAM를 통해 사용자 별 접근 가능한 서비스를 제한한다 * VPC의 보안그룹을 통해 EC2 인스턴스에 접근 가능한 위치와 수단을 정의한다. | | |
| **비고** | **..** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec306 | **이행**  **결과** | 충족 |
| **분류** | 정보시스템 접근 | 미 충족 |
| **항목명** | 정보시스템 접근에 대한 사용자 인증 통제 적용 | | |
| **요구사항 내용** | 정보시스템 및 개인정보처리시스템에 대한 접근 시 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전하게 식별하고 통제하고 있는가? | | |
| **이행**  **점검 내용** |  | | |
| **비고** | **..** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec307 | **이행**  **결과** | 충족 |
| **분류** | 정보시스템 접근 | 미 충족 |
| **항목명** | 정보시스템 접속 차단 | | |
| **요구사항 내용** | 정보시스템에 접속 후 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는가? | | |
| **이행**  **점검 내용** | * Single Sign-On를 통해 사용자가 로그온할 수 있는 시간을 설정한다. | | |
| **비고** | **..** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec308 | **이행**  **결과** | 충족 |
| **분류** | 정보시스템 접근 | 미 충족 |
| **항목명** | 서비스에 따른 독립된 서버 운영 | | |
| **요구사항 내용** | 주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가? | | |
| **이행**  **점검 내용** | * VPC를 통해 서브넷을 구분하여 WEB, WAS ,DB를 독립적으로 구성한다. | | |
| **비고** | **..** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 코드** | Sec309 | **이행**  **결과** | 충족 |
| **분류** | 정보시스템 접근 | 미 충족 |
| **항목명** | 정보시스템 관계 없는 서비스 차단 | | |
| **요구사항 내용** | 정보시스템의 사용 목적과 관련이 없거나 침해사고를 유발할 수 있는 서비스 또는 포트를 확인하여 차단하고 있는가? | | |
| **이행**  **점검 내용** | * 다음과 같이 WAS에서 Flask, SSH, 동적포트를 오픈하고 나머지 허용되지 않는 포트를 차단한다. | | |
| **비고** | **..** | | |

응용프로그램 접근

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec310 | | **이행**  **결과** | 충족 |
| **분류** | 응용프로그램 접근 | | 미 충족 |
| **항목명** | 응용프로그램 접근 권한 제한 | | | |
| **요구사항 내용** | 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근권한을 설정하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec311 | | **이행**  **결과** | 충족 |
| **분류** | 응용프로그램 접근 | | 미 충족 |
| **항목명** | 응용프로그램 중요정보의 노출 최소화 | | | |
| **요구사항 내용** | 중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec312 | | **이행**  **결과** | 충족 |
| **분류** | 응용프로그램 접근 | | 미 충족 |
| **항목명** | 응용프로그램 세션 관리 | | | |
| **요구사항 내용** | 일정 시간동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec313 | | **이행**  **결과** | 충족 |
| **분류** | 응용프로그램 접근 | | 미 충족 |
| **항목명** | 관리자 전용 응용프로그램 비인가자 접근 통제 | | | |
| **요구사항 내용** | 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 비인가자가 접근할 수 없도록 접근을 통제하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

데이터베이스 접근

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec314 | | **이행**  **결과** | 충족 |
| **분류** | 데이터베이스 접근 | | 미 충족 |
| **항목명** | 데이터베이스 접근통제 | | | |
| **요구사항 내용** | 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

원격 접근 통제

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec315 | | **이행**  **결과** | 충족 |
| **분류** | 원격접근 통제 | | 미 충족 |
| **항목명** | 단말기 접근통제 | | | |
| **요구사항 내용** | 내부 네트워크를 통하여 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근통제 하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

인터넷 접속 통제

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec316 | | **이행**  **결과** | 충족 |
| **분류** | 인터넷 접속 통제 | | 미 충족 |
| **항목명** | 외부 인터넷 접속 통제 | | | |
| **요구사항 내용** | 주요 정보시스템(DB서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec317 | | **이행**  **결과** | 충족 |
| **분류** | 인터넷 접속 통제 | | 미 충족 |
| **항목명** | 망분리 적용 및 통제 | | | |
| **요구사항 내용** | 법령에 따라 인터넷 망분리 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 망 분리를 적용하여 접근 통제하는가 ? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

보안시스템 통제

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec318 | | **이행**  **결과** | 충족 |
| **분류** | 보안시스템 통제 | | 미 충족 |
| **항목명** | 보안시스템 비인가자 접근 통제 | | | |
| **요구사항 내용** | 보안시스템 관리자 등 접근이 허용된 인원수를 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족 | | |
| **비고** | **..** | | | |

### 2.4 암호화 적용

중요정보

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec401 | | **이행**  **결과** | 충족 |
| **분류** | 중요정보 암호화 | | 미 충족 |
| **항목명** | 개인정보 및 주요정보에 대한 암호화 적용 | | | |
| **요구사항 내용** | 암호정책에 따라 개인정보 및 중요 정보의 저장, 전송, 전달 시 암호화를 수행하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

암호키 관리

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec402 | | **이행**  **결과** | 충족 |
| **분류** | 암호키 관리 | | 미 충족 |
| **항목명** | 암호키 접근권한 관리 | | | |
| **요구사항 내용** | 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

비밀번호 암호화

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec403 | | **이행**  **결과** | 충족 |
| **분류** | 비밀번호 암호화 | | 미 충족 |
| **항목명** | 비밀번호 암호화 적용 | | | |
| **요구사항 내용** | 개인정보 처리시스템 저장시 암호화 적용을 하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

### 2.5 로깅 및 모니터링

로그관리

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec501 | | **이행**  **결과** | 충족 |
| **분류** | 로그 관리 | | 미 충족 |
| **항목명** | 로그 기록 보관 및 관리 | | | |
| **요구사항 내용** | 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그를 보관 및 관리를 하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec502 | | **이행**  **결과** | 충족 |
| **분류** | 로그 관리 | | 미 충족 |
| **항목명** | 로그 기록 접근권한 설정 | | | |
| **요구사항 내용** | 정보시스템의 로그기록에 대한 접근권한은 최소화하여 부여하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec503 | | **이행**  **결과** | 충족 |
| **분류** | 로그 관리 | | 미 충족 |
| **항목명** | 정보시스템 이상징후 인지를 위한 모니터링 절차 이행 | | | |
| **요구사항 내용** | 정보시스템 관련 오류, 오‧남용(비인가접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 절차를 수립‧이행하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec504 | | **이행**  **결과** | 충족 |
| **분류** | 로그 관리 | | 미 충족 |
| **항목명** | 로그 시간 동기화 | | | |
| **요구사항 내용** | 로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 각 정보시스템의 시간을 표준시간으로 동기화하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec505 | | **이행**  **결과** | 충족 |
| **분류** | 로그 관리 | | 미 충족 |
| **항목명** | 이상행위 발생 시 신속한 분석 및 점검 | | | |
| **요구사항 내용** | 내‧외부에 의한 침해시도, 개인정보 유출 시도, 부정행위 등 이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

### 2.6 보안관리

시험과 운영 환경 분리

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec601 | | **이행**  **결과** | 충족 |
| **분류** | 시험과 운영 환경 분리 | | 미 충족 |
| **항목명** | 시험 시스템과 운영시스템의 분리 | | | |
| **요구사항 내용** | 정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

시험 데이터 보안

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec602 | | **이행**  **결과** | 충족 |
| **분류** | 시험 데이터 보안 | | 미 충족 |
| **항목명** | 실제 운영 데이터의 사용 제한 | | | |
| **요구사항 내용** | 정보시스템의 개발 및 시험 과정에서 실제 운영 데이터의 사용을 제한하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

장애 관리

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec603 | | **이행**  **결과** | 충족 |
| **분류** | 장애 관리 | | 미 충족 |
| **항목명** | 정보시스템의 장애 관리 | | | |
| **요구사항 내용** | 정보시스템의 장애를 인지하고 탐지 및 관리를 하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

클라우드 보안

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec604 | | **이행**  **결과** | 충족 |
| **분류** | 클라우드 보안 | | 미 충족 |
| **항목명** | 클라우드 서비스 보안 통제 정책 이행 | | | |
| **요구사항 내용** | 클라우드 서비스 이용 시 비인가 접근, 설정오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 이행하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec605 | | **이행**  **결과** | 충족 |
| **분류** | 클라우드 보안 | | 미 충족 |
| **항목명** | 클라우드 서비스 관리자 권한 보호대책 적용 | | | |
| **요구사항 내용** | 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가된 접근, 권한 오남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호대책을 적용하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

공개서버 보안

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec606 | | **이행**  **결과** | 충족 |
| **분류** | 공개서버 보안 | | 미 충족 |
| **항목명** | 공개서버 DMZ 설치 및 보안시스템 보호 | | | |
| **요구사항 내용** | 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

패치관리

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec607 | | **이행**  **결과** | 충족 |
| **분류** | 패치관리 | | 미 충족 |
| **항목명** | 공개 인터넷 접속을 통한 패치 제한 | | | |
| **요구사항 내용** | 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

악성코드 통제

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec608 | | **이행**  **결과** | 충족 |
| **분류** | 악성코드 통제 | | 미 충족 |
| **항목명** | 악성코드 보호대책 이행 | | | |
| **요구사항 내용** | 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용단말기 등을 보호하기 위하여 보호대책을 이행하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec609 | | **이행**  **결과** | 충족 |
| **분류** | 악성코드 통제 | | 미 충족 |
| **항목명** | 악성코드 대응절차 이행 | | | |
| **요구사항 내용** | 악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응절차를 이행하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |

### 2.7 개인정보보호

개인정보보호

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **보안 코드** | Sec701 | | **이행**  **결과** | 충족 |
| **분류** | 개인정보보호 | | 미 충족 |
| **항목명** | 개인정보처리시스템 법률 준수 검토 및 관리 | | | |
| **요구사항 내용** | 개인정보처리시스템에 대한 접속기록은 법적 요구사항을 준수할 수 있도록 관리하고 있는가? | | | |
| **이행**  **점검 내용** | 충족 | 미충족  - | | |
| **비고** | **..** | | | |